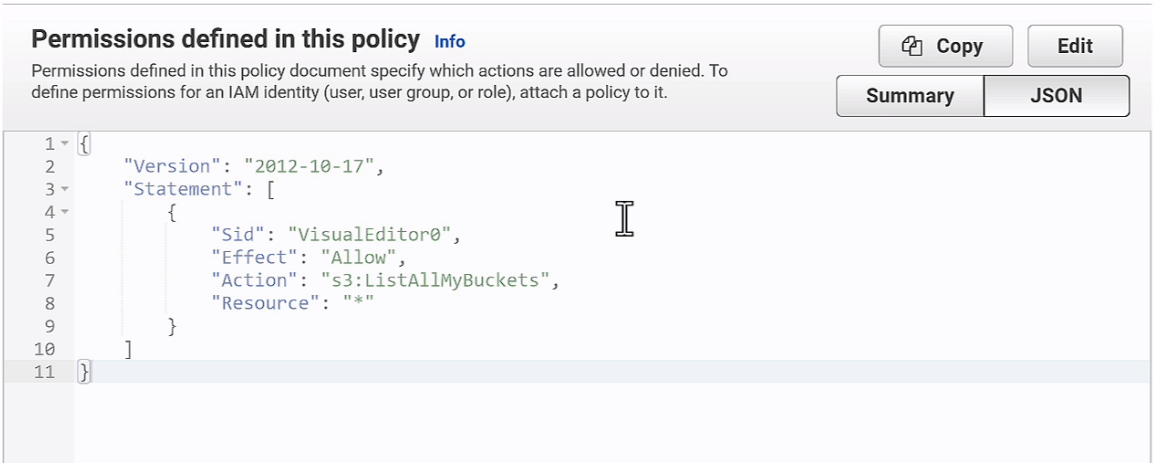
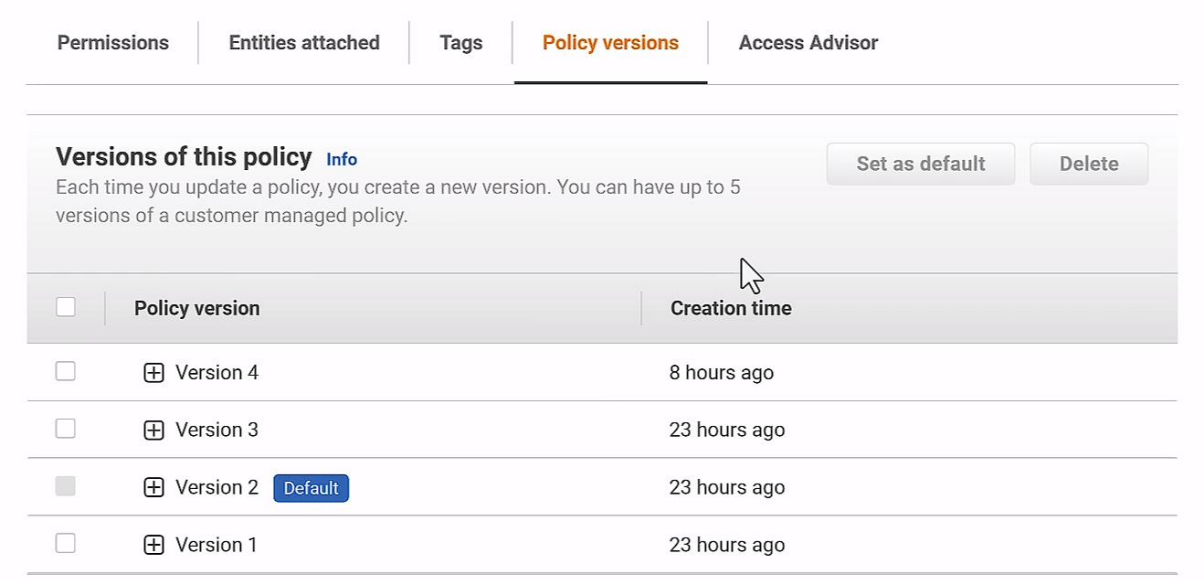
😊 ACCESS TO S3 BUCKET FROM ANOTHER ACCOUNT

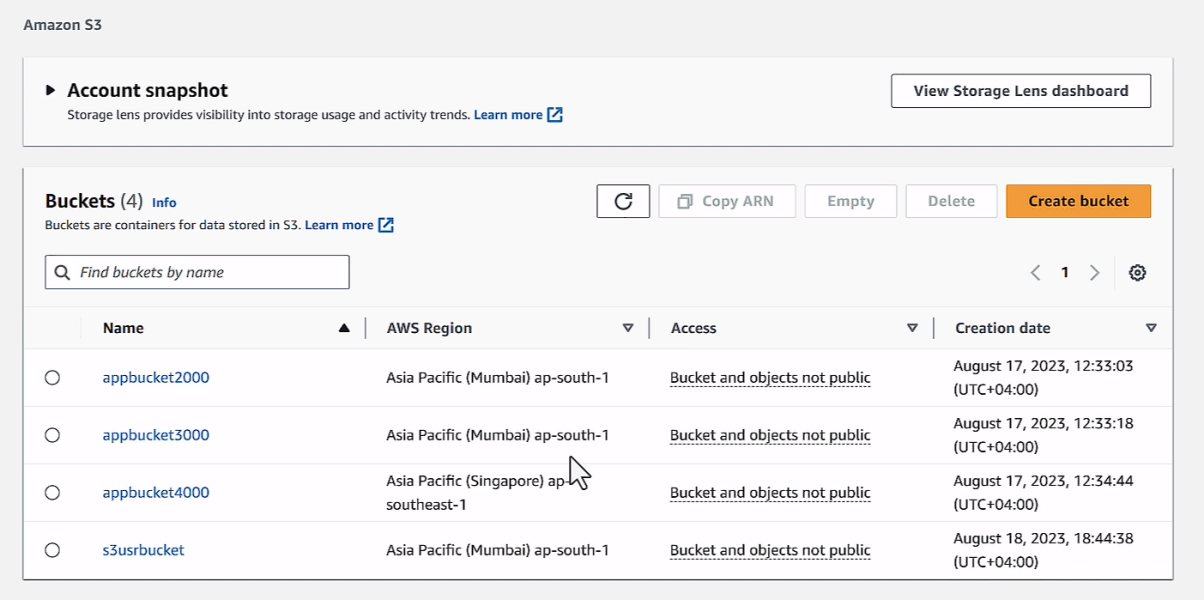
1. In this lab you have to use two accounts in order to access the S3 bucket and its objects.
2. Now you need to login with both of them in different browser.
3. You are going to command prompt, because this is how will access the buckets.
4. With that you need to create some policies to give access 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.



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



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



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.

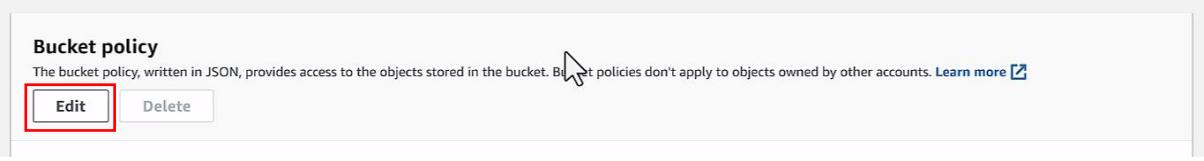
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountBucketAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::appbucket4000",
        "arn:aws:s3:::appbucket4000/*"
      ]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

]

}

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.

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



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": "AllowobjectAccesstos3user",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::213171387512:user/s3-usr01"
            },
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::appbucket4000/*"
            ]
```

```
            },
            {
                "Sid": "AllowbucketAccesstos3user",
                "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>
```