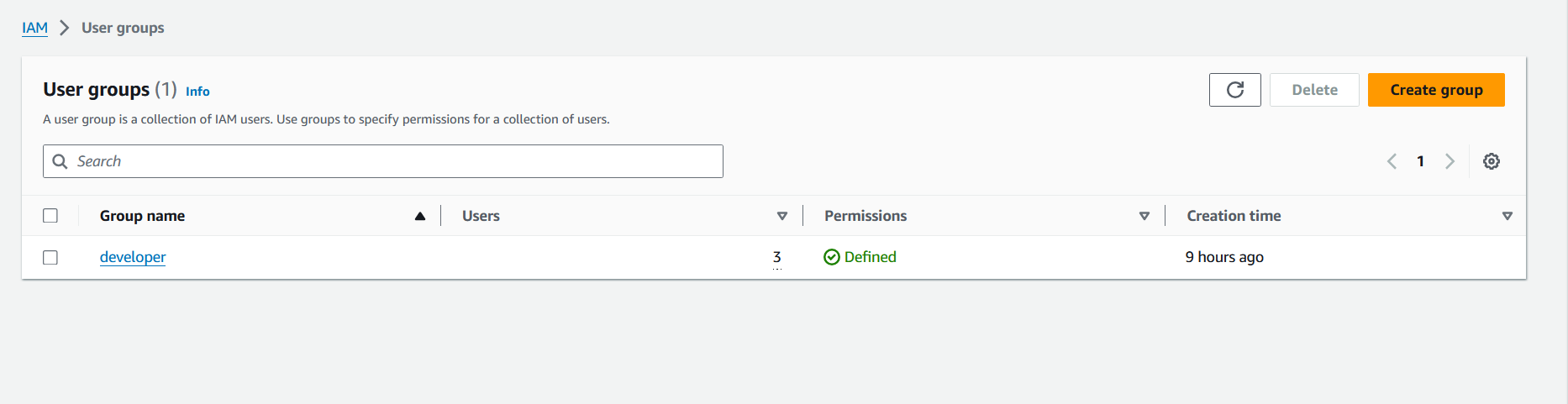
22. Create developers group

 Go to the **IAM** service in the AWS Management Console.

 On the left-hand menu, select **Groups**, then click **Create group**.

 Enter **Developers** as the group name.

 Skip attaching any policies for now (you’ll attach them later). Click **Create group**.



23. create usera with immediate change of password when login and addd this user to develoeprs group

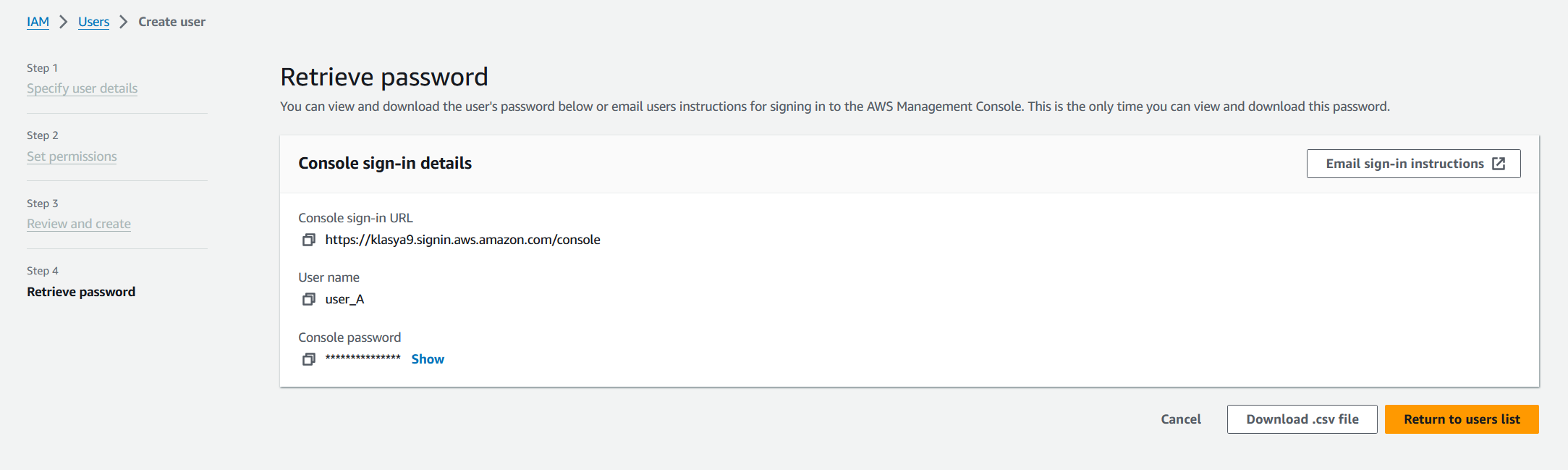
 Go to **Users** in the IAM dashboard, and click **Add user**.

 Enter the username as usera.

 Select **Password - AWS Management Console access**, and check the option **Require password reset**.

 Click **Next** to set permissions.

 In the **Set permissions** step, choose **Add user to group** and select the **Developers** group.

 Click **Next: Review**, and then **Create user**.

24. Create a policy s3 readonly access and attach to develoeprs group

 In the IAM Console, navigate to **Policies** from the left-hand menu, then click **Create Policy**.

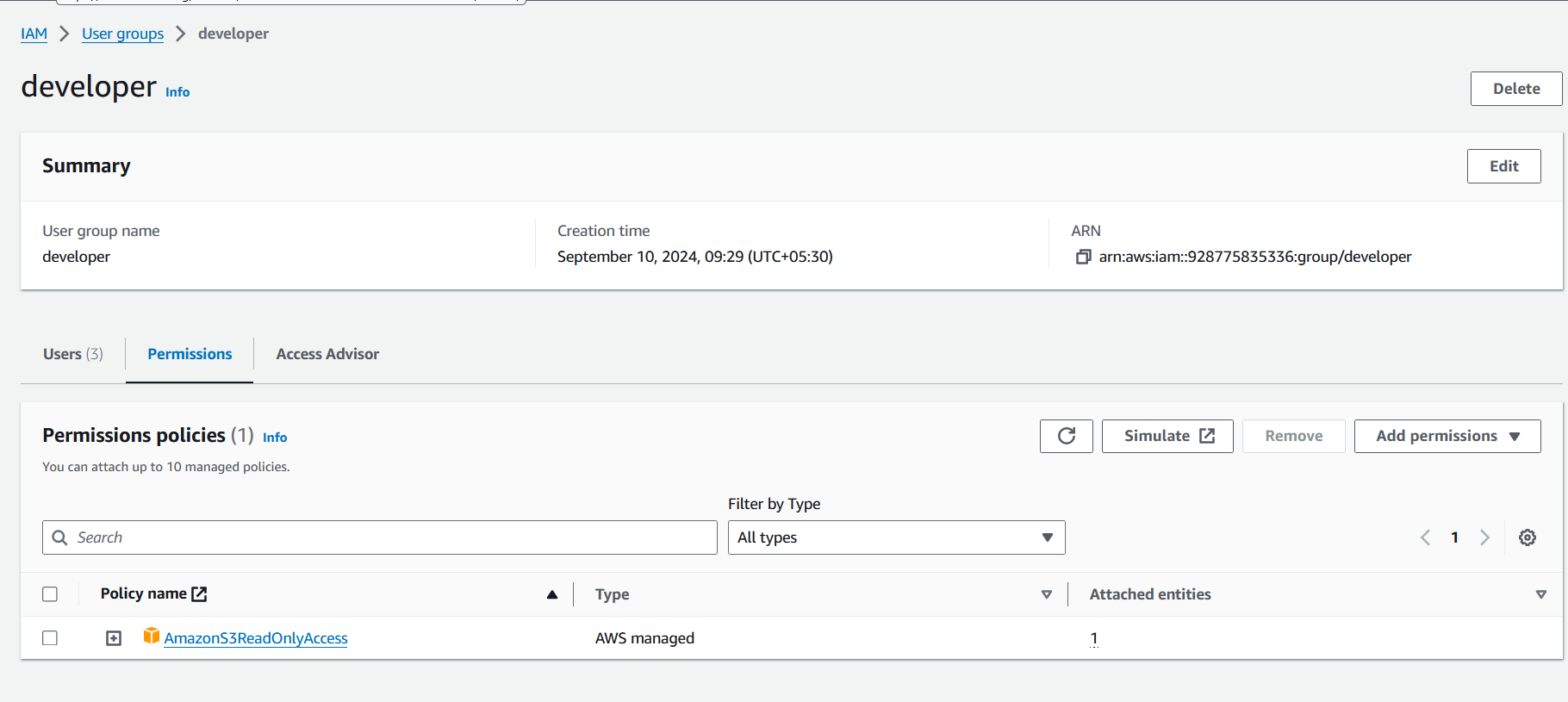
 Use the **Visual editor**:

* Select **Service**: S3.
* Select **Actions**: Under **Read**, choose **ListBucket**, **GetObject**, etc.
* Select **Resources**: Choose either **All resources** or specify specific buckets and objects.

 Review the policy and give it a name like S3ReadOnlyPolicy.

 Click **Create policy**.

 Go to **Groups** → Select **Developers** → Click **Add permissions** → Choose the policy you just created and attach it to the group.



25. login with usera and verify he has only s3 read-only access

 **ogin as usera**: Go to the AWS sign-in page, enter the IAM username usera, and the temporary password.

 You will be prompted to reset the password.

 Once logged in, navigate to the **S3** service:

* You should be able to list buckets and view contents but not modify or delete any objects.

 Try any unauthorized action (e.g., deleting an object) to confirm read-only permissions.

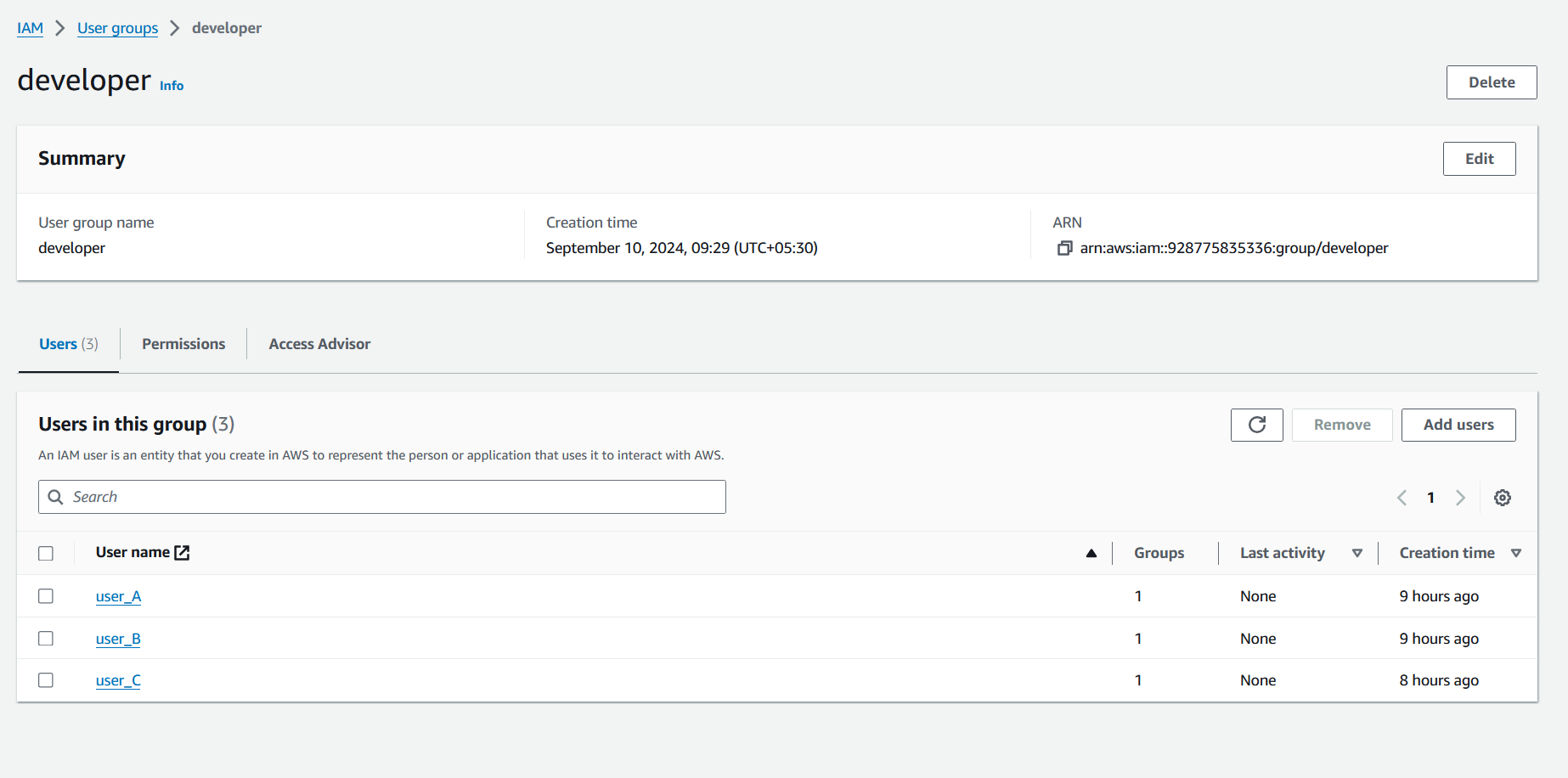
26. Create userb

 Go to **IAM** → **Users** → **Add user**.

 Enter the username userb.

 Select **Password** for AWS Management Console access and continue without requiring a password change.

 Click **Next: Review** and create the user.



27. Create ec2 full access and s3 full access policy and attached that policy to user-b

Go to IAM → Policies → Create Policy.

EC2 Full Access:

Select Service: EC2.

Under Actions, choose All EC2 actions.

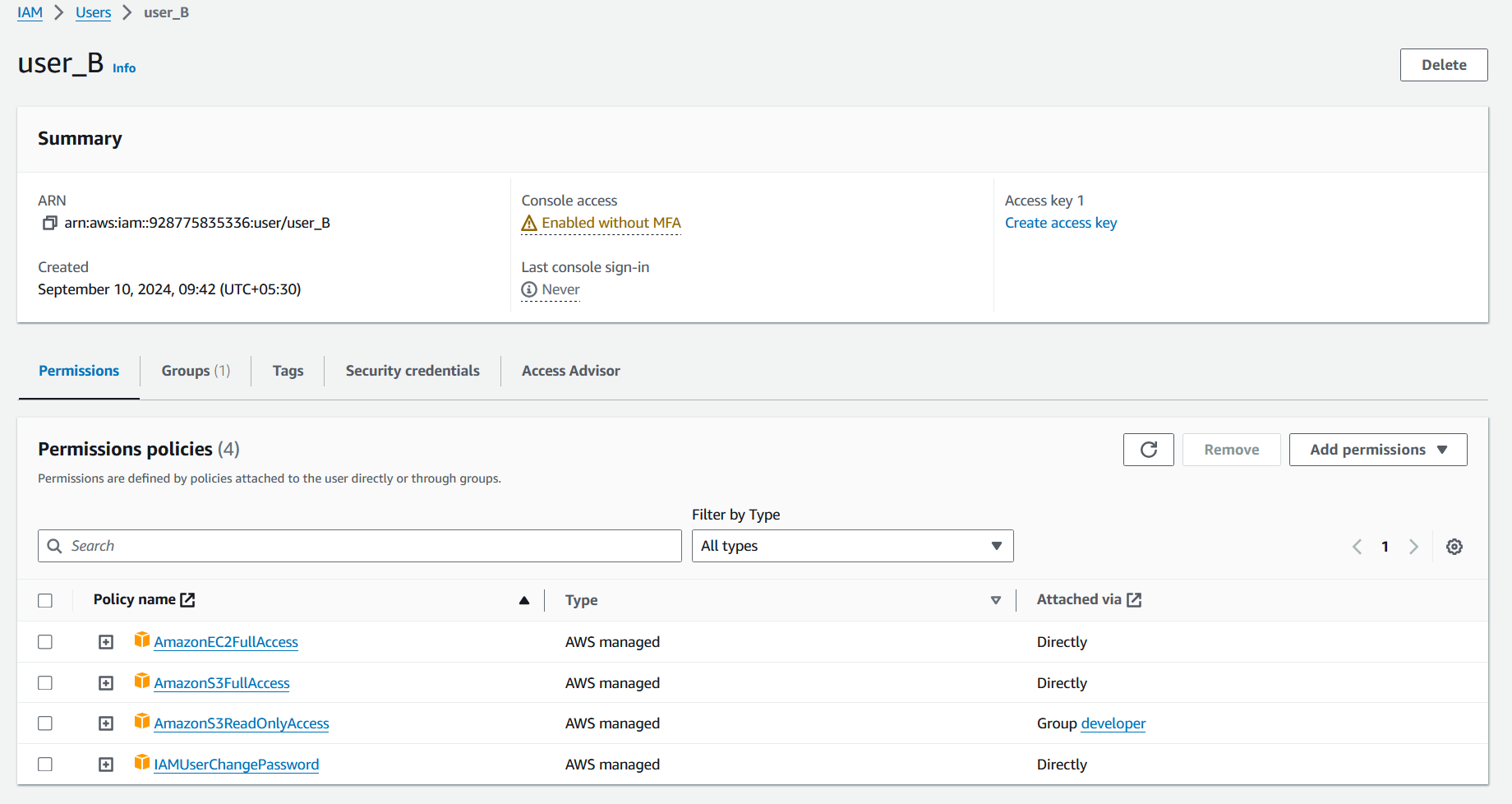
S3 Full Access:

Select Service: S3.

Choose All S3 actions.

Review the policy, name it EC2AndS3FullAccess, and create it.

Go to Users → userb → Permissions tab → Add permissions → Attach the new EC2AndS3FullAccess policy to userb.

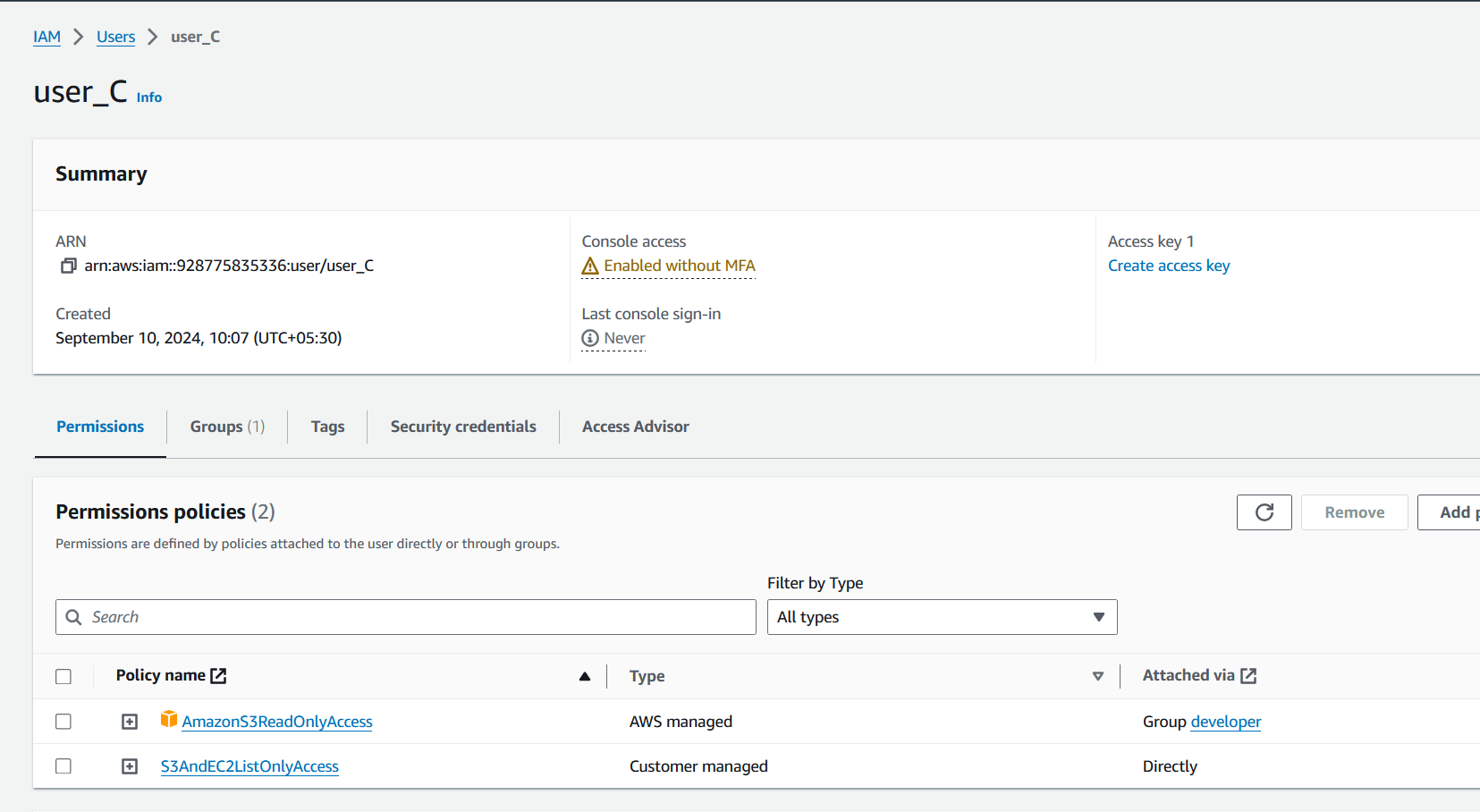


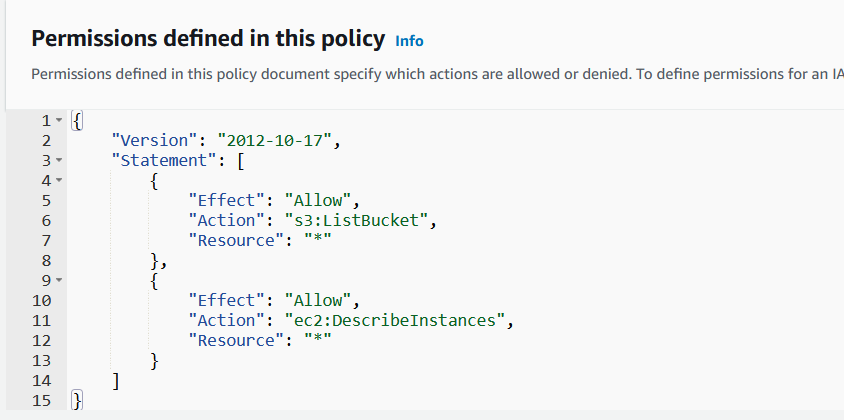
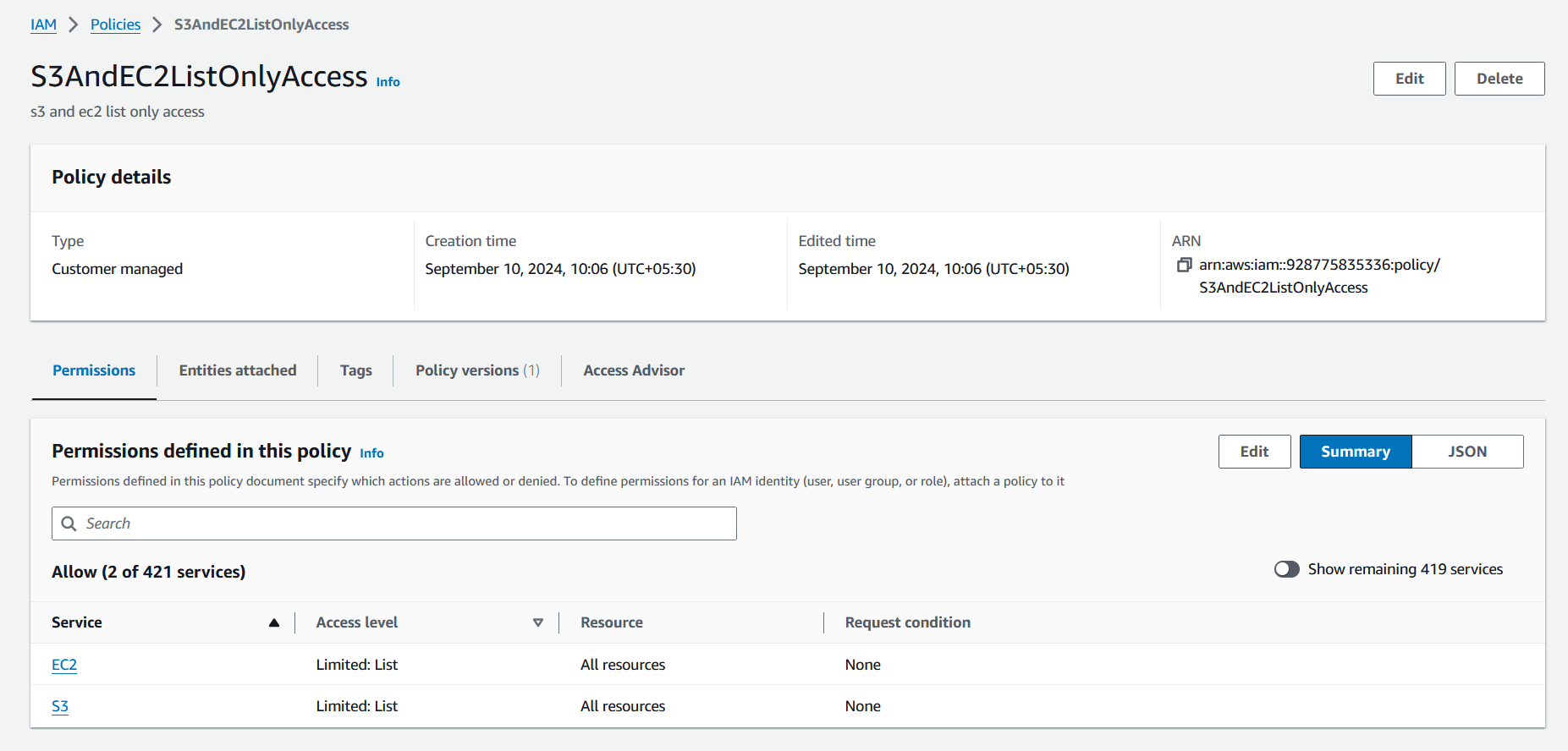
28. verify user has ec2,s3 full aceess via console

1. Log in as userb using the password.
2. Navigate to **S3**:
   * You should be able to list, create, and delete buckets.
   * Try creating a new bucket to confirm full access.
3. Navigate to **EC2**:
   * You should be able to launch, stop, and terminate instances.

**29. Create List-Only S3 + EC2 Access for userc Using Policy Creator UI**

1. **Create User userc**:
   * Go to **IAM** → **Users** → **Add user**.
   * Enter the username userc and create it with password access.
2. **Create a List-Only Policy**:
   * Go to **IAM** → **Policies** → **Create Policy**.
   * **S3 List-Only**:
     + Select **Service**: S3.
     + Select **Actions**: Only choose **ListBucket** under **List**.
     + Select **Resources**: All resources.
   * **EC2 List-Only**:
     + Select **Service**: EC2.
     + Select **Actions**: Only choose **DescribeInstances**.
     + Select **Resources**: All resources.
   * Name the policy S3AndEC2ListOnlyAccess and create it.
3. **Attach the Policy to userc**:
   * Go to **Users** → **userc** → **Permissions** tab → **Add permissions**.
   * Search for S3AndEC2ListOnlyAccess and attach it to userc.
4. **Verify userc's Access**:
   * Login as userc in the AWS console.
   * Go to **S3**: You should only be able to list buckets, not modify or delete.
   * Go to **EC2**: You should only be able to view instance details without performing any modifications.

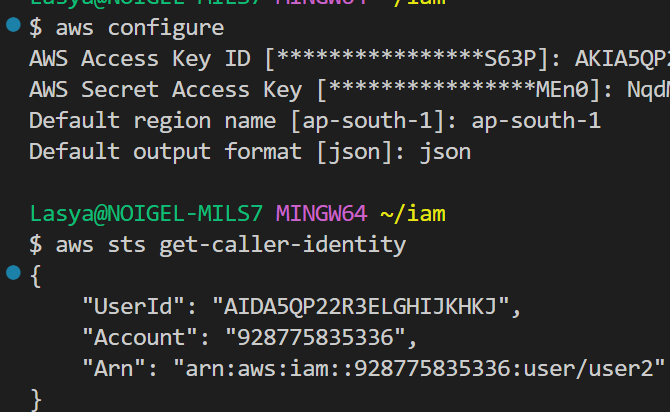




30. create accesskey and secret keys and configure aws cli on windows local machine

31. run aws configure command it will ask for ur access/secret keys and then u will get access to your aws cloud from your local.







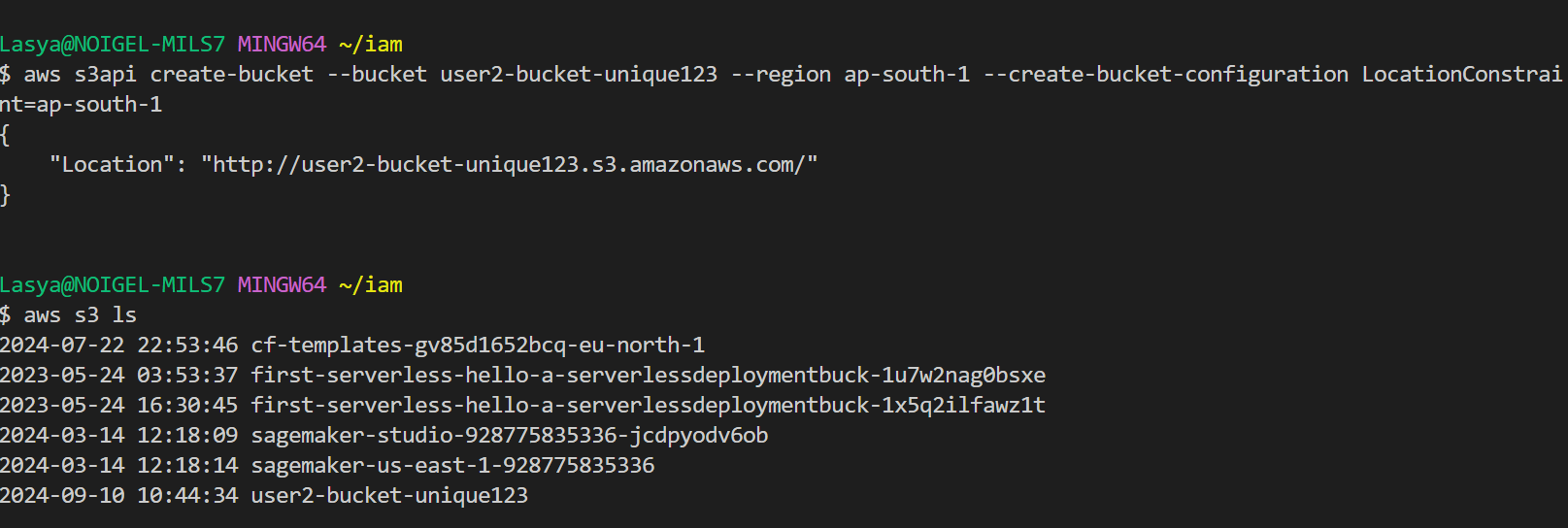
which mean you can do all operations form aws cli.

32. create s3 bucket using aws cli

aws s3api create-bucket --bucket bubucke --region ap-south-1 --create-bucket-configuration LocationConstraint=ap-south-1

faced the prob of locationconstraint

33. create ec2 instance using aws cli



aws ec2 describe-images --owners amazon

aws ec2 describe-key-pairs --region ap-south-1

aws ec2 run-instances --image-id ami-0a235a40f3e7f88d1 --count 1 --instance-type t2.micro --key-name shdregf --region ap-south-1

33. create iam user using aws cli

aws iam create-user --user-name iamcliuser\_A



34. create policy using aws cli

S3.json

{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Effect": "Allow",

            "Action": "s3:ListBucket",

            "Resource": "arn:aws:s3:::user2-bucket-unique123"

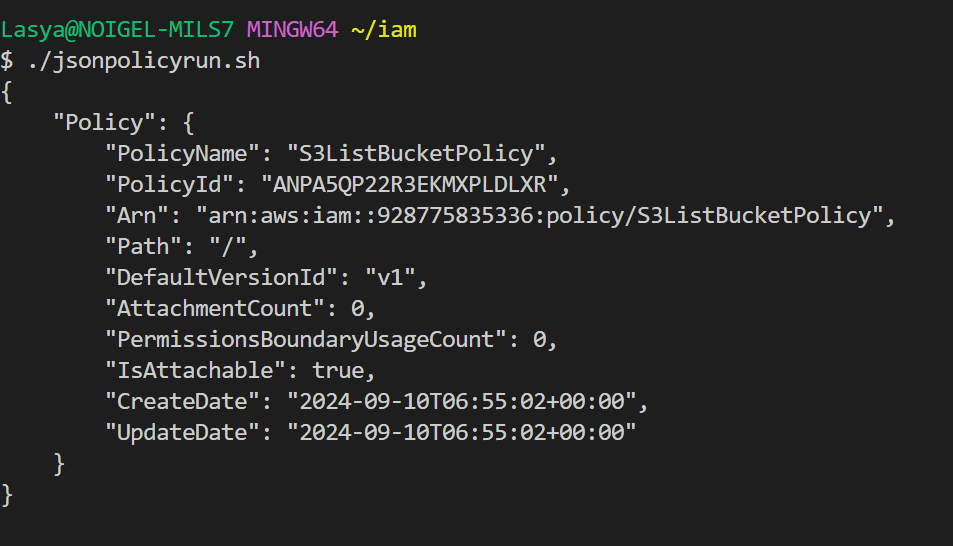
        }

    ]

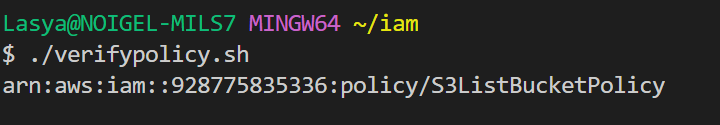
}

aws iam create-policy --policy-name S3ListBucketPolicy --policy-document <file://s3.json>

<file://ec2-full-access-policy.json>



aws iam list-policies --query "Policies[?PolicyName=='S3ListBucketPolicy'].Arn" --output text



35. attach policy to user using aws cli

aws iam attach-user-policy --user-name iamcliuser\_A --policy-arn arn:aws:iam::928775835336:policy/S3ListBucketPolicy

