**Lab Steps**

**Task 1: Sign in to AWS Management Console**

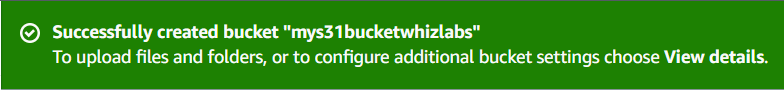
1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
   * Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
   * Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1.**

**Task 2: Creating a S3 Bucket**

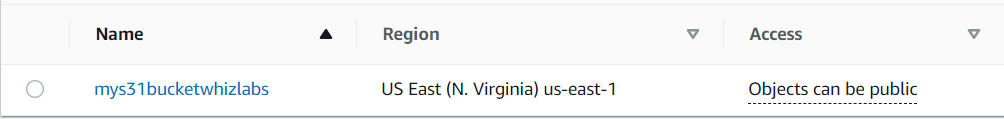
In this task, we are going to create a S3 bucket by providing the required configurations such as name, region and ACLs.

1. Ensure you are in the **US East (N. Virginia) us-east-1**Region to begin creating an S3 bucket in the Amazon cloud.
2. Navigate to the **Services**menu at the top. Click on **S3** in the **Storage** section.
3. On the S3 Page, click on **Create bucket**and fill in the bucket details.
   * Bucket name: Enter**mys3bucketlabs-test**
     + **Note:**S3 bucket name is globally unique, choose a name that is available.
   * AWS Region: Select **US East (N. Virginia) us-east-1**
   * For Object ownership: Select **ACLs disabled**

* For **Block Public Access settings for this bucket** for this bucket section,
  + Uncheck the option**, Block all public access,**
    - **Check** the **I acknowledge that the current settings might result in this bucket and the objects within becoming public** checkbox.
* Leave other settings as default.
* Click on **Create bucket**button.

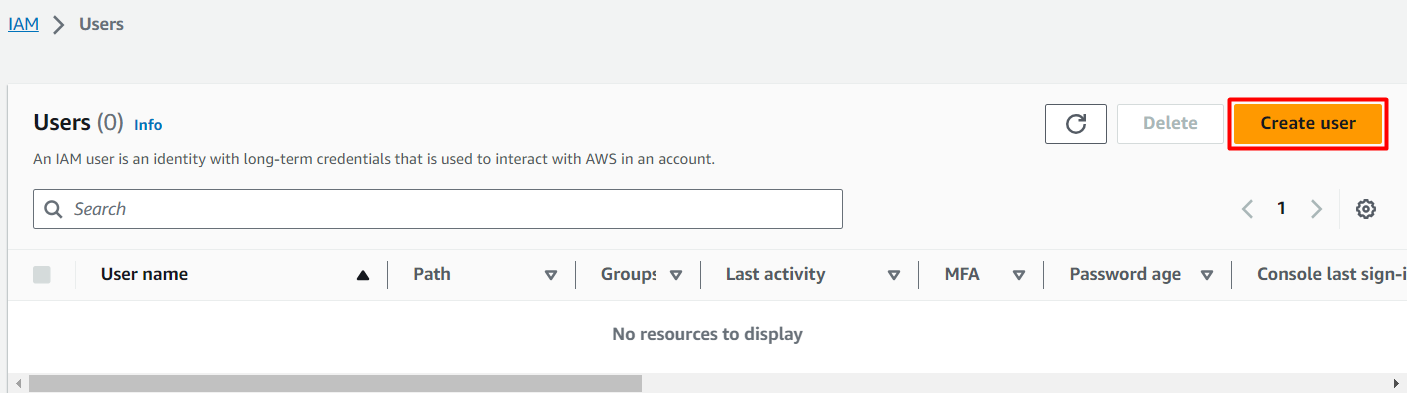


1. The S3 bucket will be created successfully.



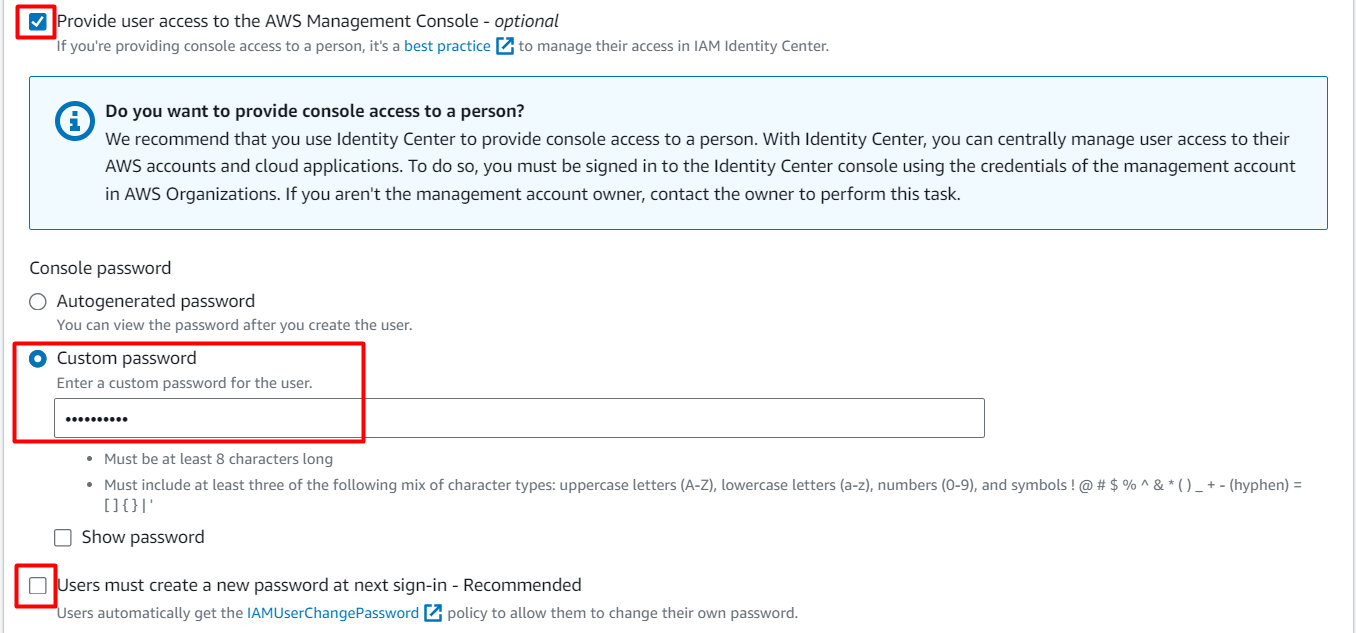
**Task 3: Creating an IAM user using Console**

1. Click on **Services** and select **IAM** under the **Security, Identity, & Compliance** section.
2. Navigate to the **Users** in the left panel and click on the **Create user** to create a new IAM user.



     3. In **Specify User Details**page,

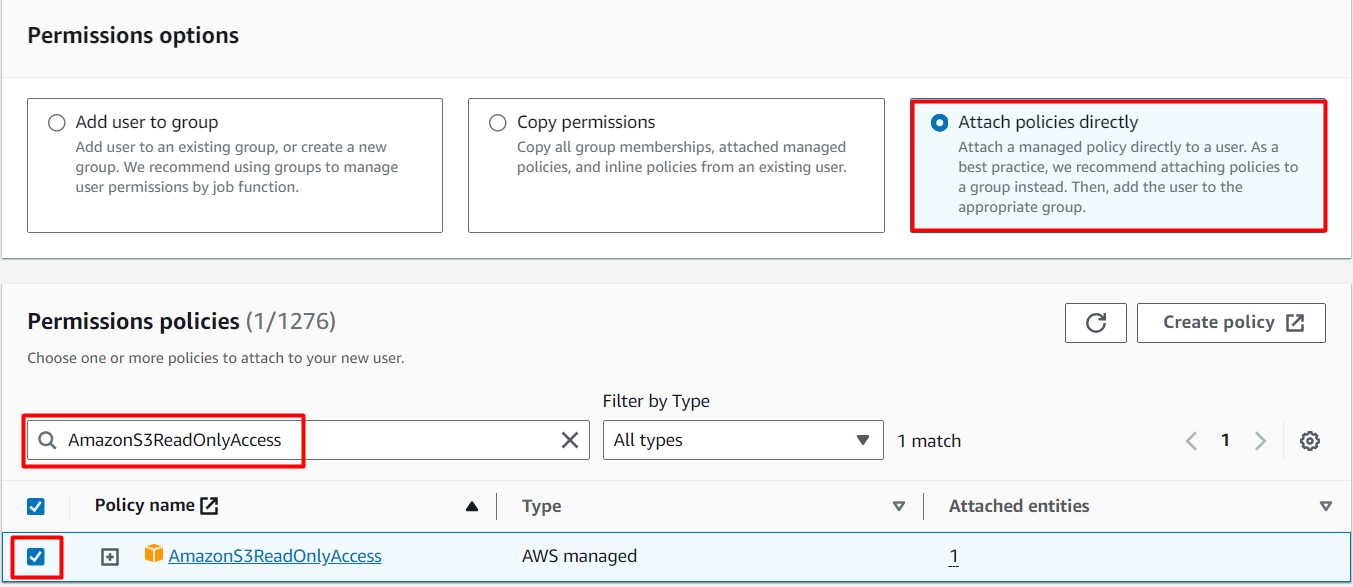
* In User name: Enter **<YOUR\_NAME>**
* Check the **Provide user access to the AWS Management Console - optional** checkbox
* Choose **Custom Password**under Console Password.   
    
  + Enter any password for e.g. **Whizlabs@123**
* Uncheck the **Users must create a new password at next sign-in - Recommended** checkbox.



* Click on **Next**button.

     4. Select **Attach policies directly**from the Permission options.

* Search for **AmazonS3ReadOnlyAccess**and select it.



     5. Review the details and click on the **Create user**button.

     6. Click on **Download .csv file (** An Excel file having details of user)

     7. Copy the **Console login link** and paste it in a different browser or incognito window.

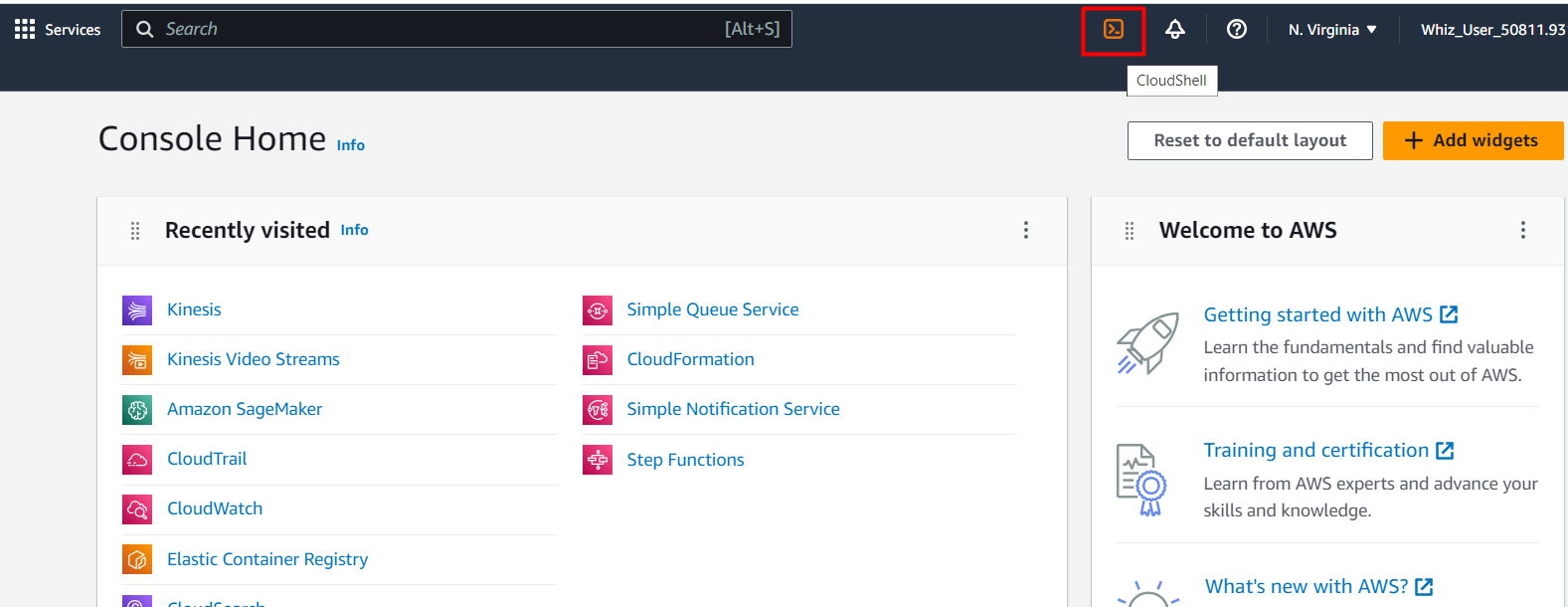
      8. Enter the IAM User Name and password you have set while creating the user and you can see that you will be successfully logged in.

**Task 4: Testing IAM user**

1. After the successful login, make sure you are in the **US East (N. Virginia) us-east-1**Region.
2. Navigate to the **Services** menu at the top. Click on **S3** in the **Storage** section.
3. You can see the bucket created in the user account.
4. Navigate to the **Services**menu at the top. Click on **EC2**in the **Compute**section.
5. Navigate to the **Instances**in the left navigation panel. You can see that you are not authorized to view all the instances because we have not added the EC2ReadAccess policy.

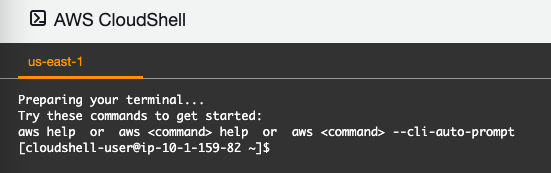
**Task 5: Create an Environment in CloudShell**

1. ?Make sure you are in the **N.Virginia** Region.
2. Navigate back to the **root** account (**Whiz\_user\_<RandomNumber>**).
3. Click on the **Cloud Shell icon**on the top right AWS menu bar.



     3. You will see a creating environment message on the screen.

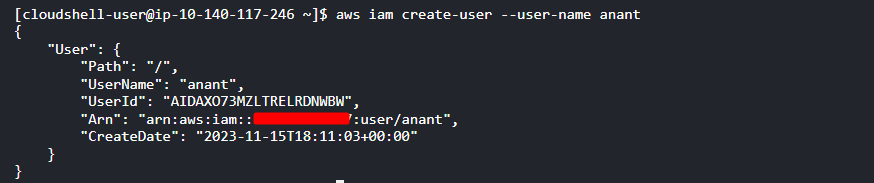
     4. Wait for a few minutes to complete the environment creation. Once the environment is created, You are ready to use the terminal.



**Task 6: Create an IAM User using CLI (Cloudshell)**

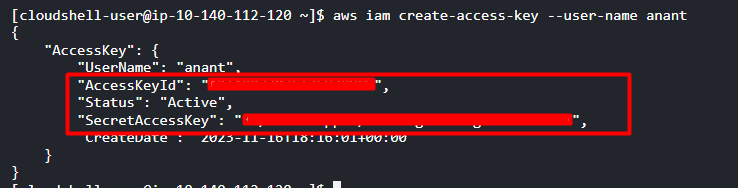
1. To create an IAM user using CLI, copy and paste the below command:

aws iam create-user --user-name <your\_username>



   2. To create the access key and secret key for the user anant, paste the following command. Remember to copy the Access Key and Secret Access Key in the notepad.

aws iam create-access-key --user-name <your\_username>

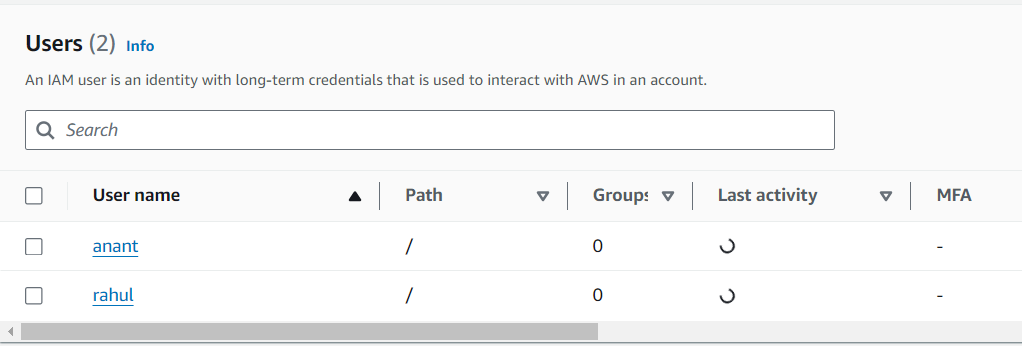


   3. Use the following command to attach the AWSS3ReadAccess policy with the user

aws iam attach-user-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess --user-name <your\_username>

   4. Click on **Services** and select **IAM** under the **Security, Identity, & Compliance** section.

   5. Navigate to the **Users** in the left panel and you can view the user created using CLI.



   6. To access the user, use the below command to access the user:

aws configure

   7. You will be asked for the access key and secret access key. Paste the keys copied earlier. Press [ENTER] after pasting the keys.

* For Default region name: Enter **us-east-1**
* For output: Press **[ENTER]**

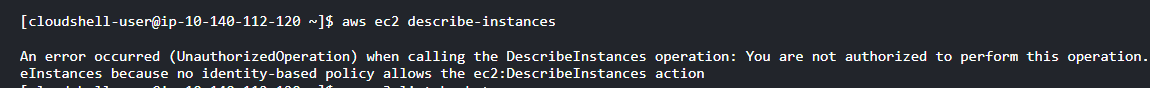
   8. To access the S3 bucket you created, paste the below command:

aws s3 ls

9. You can see the bucket you created. You are authorized to access this because you have added the S3 Read policy with the user.

 10. If you try to access any other services for e.g EC2 , you will not be authorized. Use the below command to check the same:

aws ec2 describe-instances



**Do You Know ?**

By granting IAM users access to both the Console and CloudShell, you provide them with a comprehensive toolkit for managing AWS resources efficiently and effectively. This approach can enhance productivity, streamline workflows, and empower users to tackle a wider range of tasks.