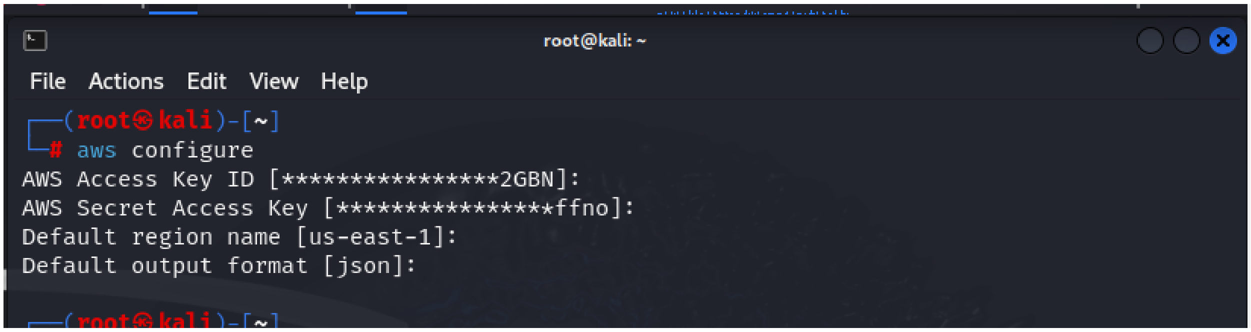
Identity and Access Management (IAM) lab

1. Open the Environment on CLI

Start by ensuring you are using the AWS CLI in a terminal environment. Make sure the AWS CLI is installed and properly configured with the correct AWS credentials and region.

- Open Terminal
- Configure AWS CLI
  - Provide the necessary inputs for:
  - AWS Access Key ID
  - AWS Secret Access Key
  - Default region name (e.g., us-east-1)
  - Default output format (e.g., json)

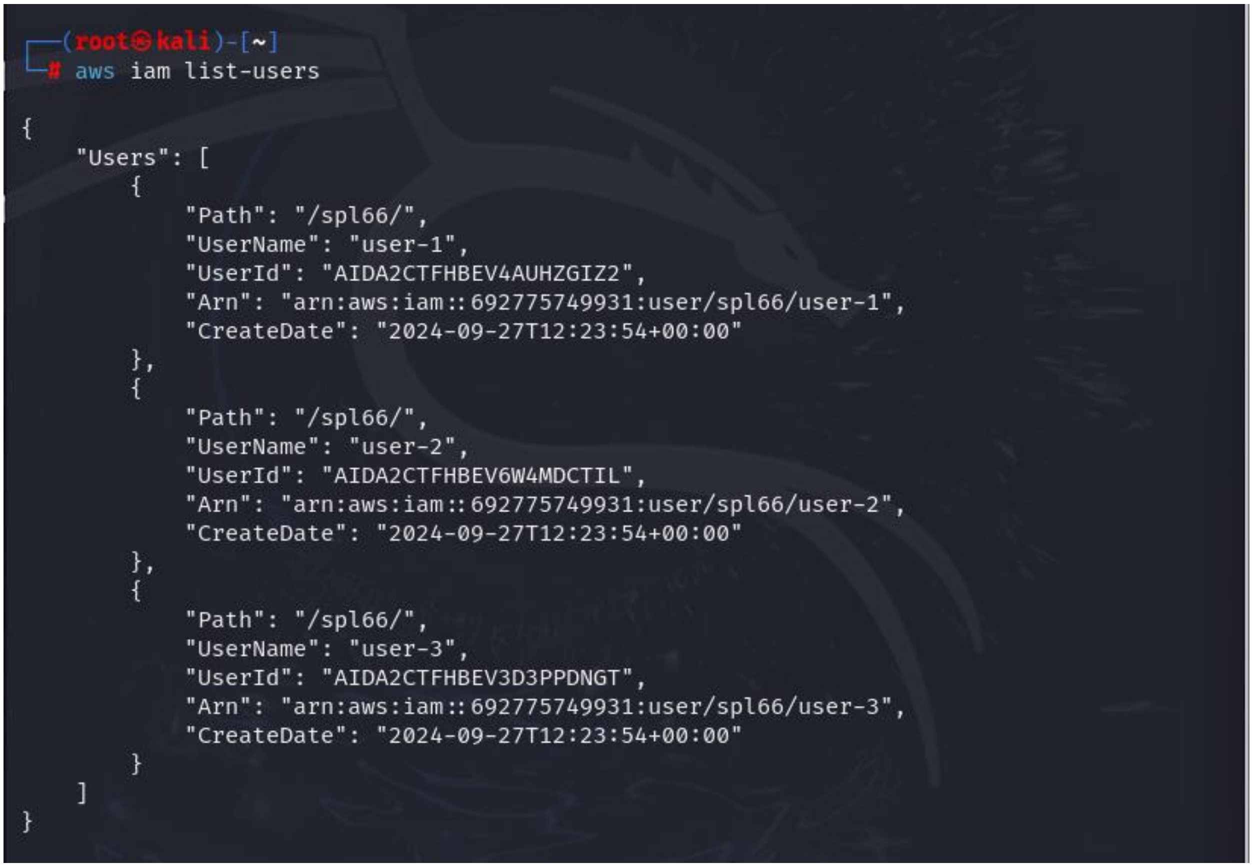


```
┌──(root㉿kali)-[~]
└─# aws configure
AWS Access Key ID [****************2GBN]:
AWS Secret Access Key [****************ffno]:
Default region name [us-east-1]:
Default output format [json]:

┌──(root㉿kali)-[~]
```

2. Task 1: Explore Users and Groups

Step 1: List IAM Users

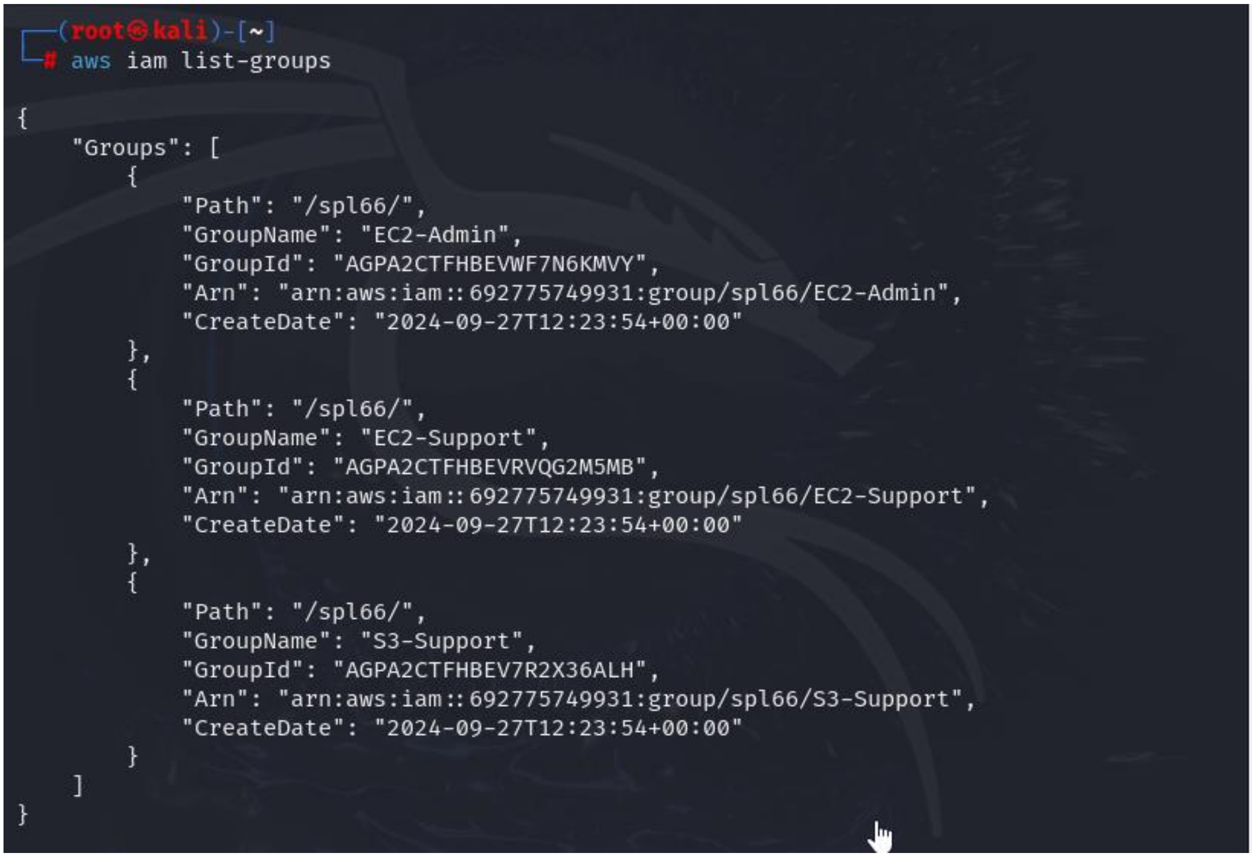
List all the IAM users to get an overview of pre-created users.



```
┌──(root㉿kali)-[~]
└─# aws iam list-users

{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA2CTFHBEV6W4MDCTIL",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA2CTFHBEV3D3PPDNGT",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ]
}
```

Step 2: List IAM Groups

Retrieve a list of all IAM groups.

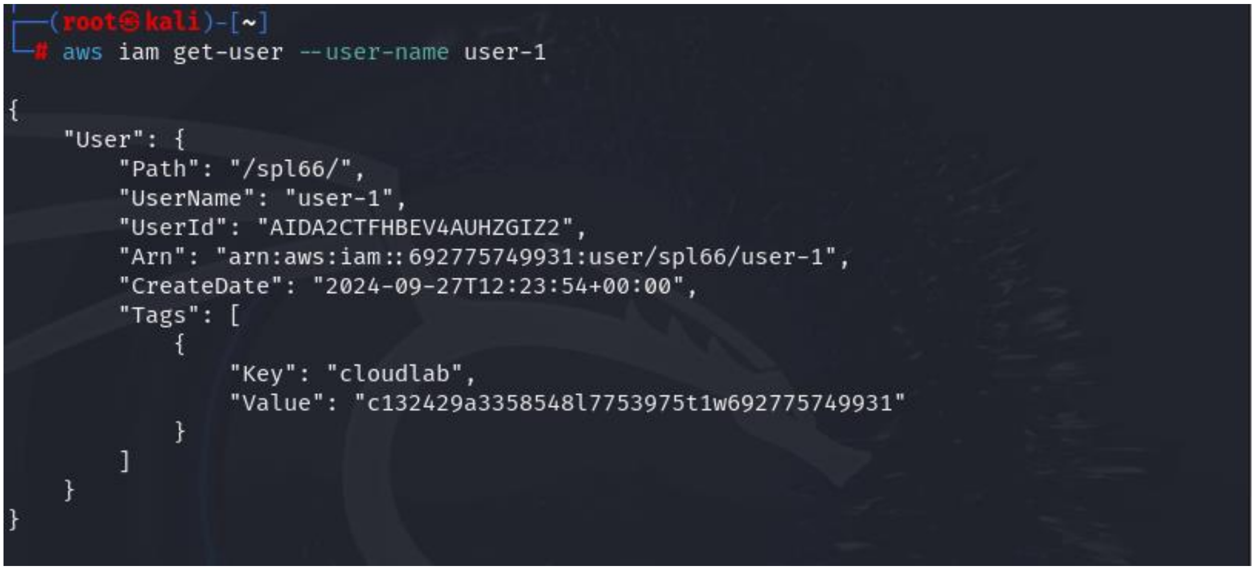


```
┌──(root㉿kali)-[~]
└─# aws iam list-groups

{
    "Groups": [
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Admin",
            "GroupId": "AGPA2CTFHBEVWF7N6KMVY",
            "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "EC2-Support",
            "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
            "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        },
        {
            "Path": "/spl66/",
            "GroupName": "S3-Support",
            "GroupId": "AGPA2CTFHBEV7R2X36ALH",
            "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ]
}
```

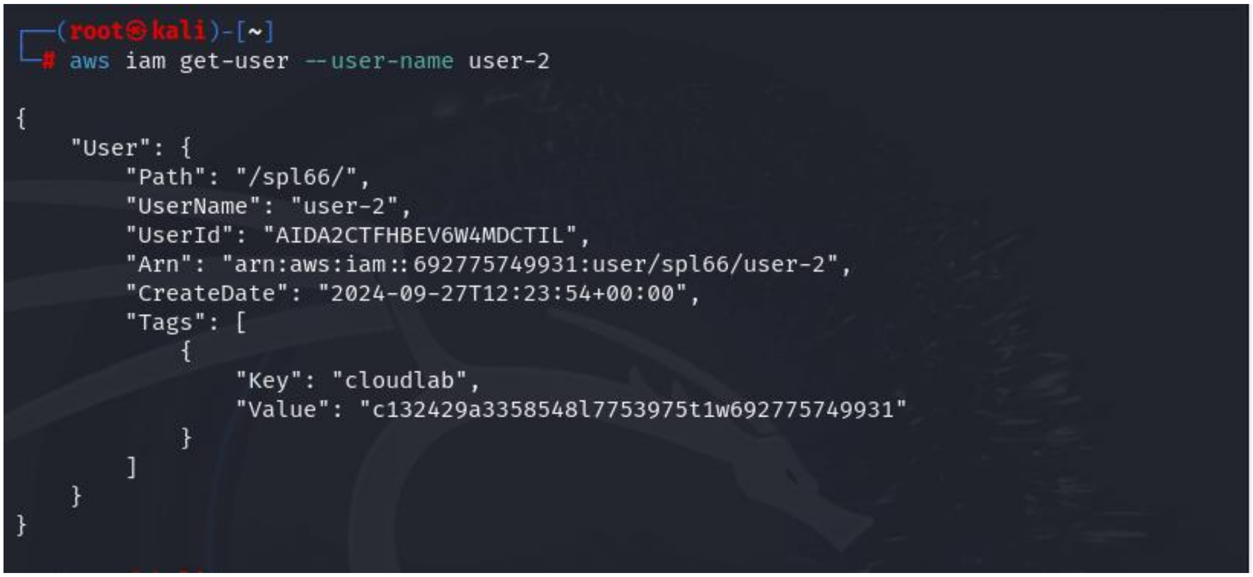
Step 3: View User Details

To inspect a specific user, use the following command by replacing <user_name> with the actual username.

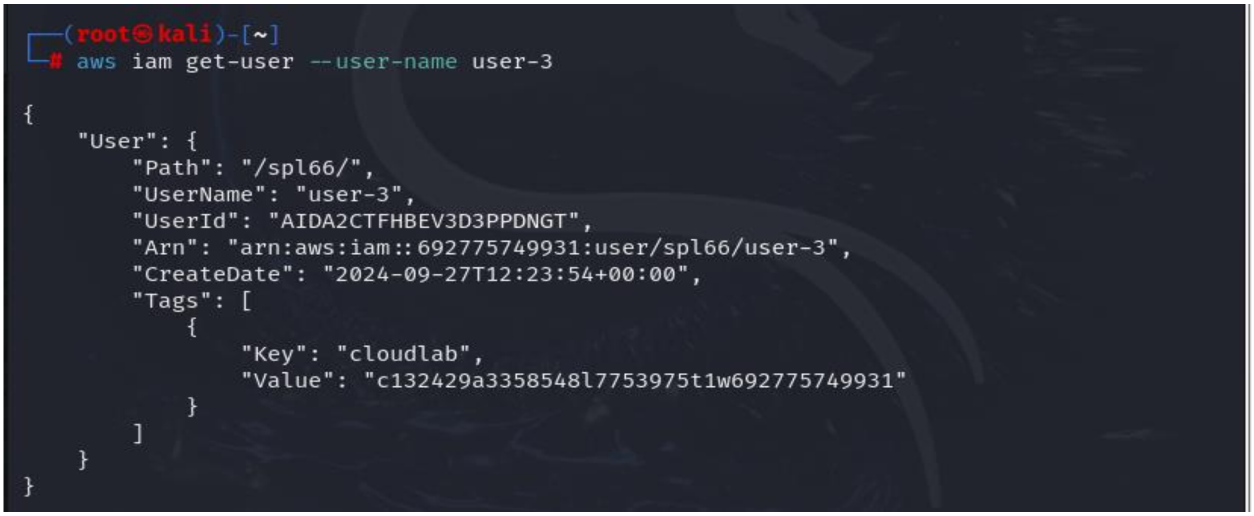
aws iam get-user --user-name <user_name>



```
┌──(root㉿kali)-[~]
└─# aws iam get-user --user-name user-1

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-1",
        "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```



```
┌──(root㉿kali)-[~]
└─# aws iam get-user --user-name user-2

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-2",
        "UserId": "AIDA2CTFHBEV6W4MDCTIL",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```

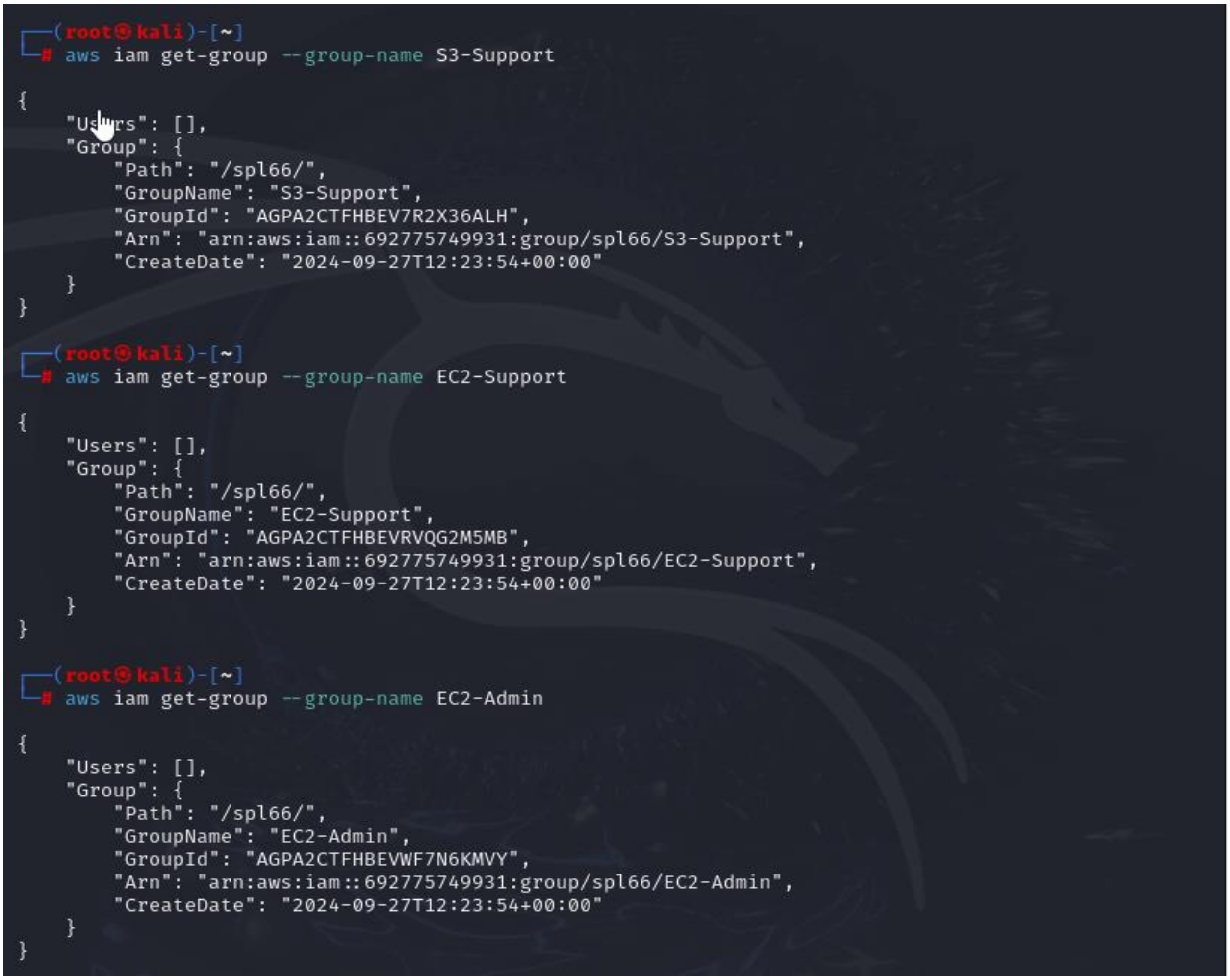


```
┌──(root㉿kali)-[~]
└─# aws iam get-user --user-name user-3

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDA2CTFHBEV3D3PPDNGT",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```

Step 4: List Users in a Specific Group

To get a list of all users that belong to a specific group, replace <group_name> with the group name.

aws iam get-group --group-name <group_name>

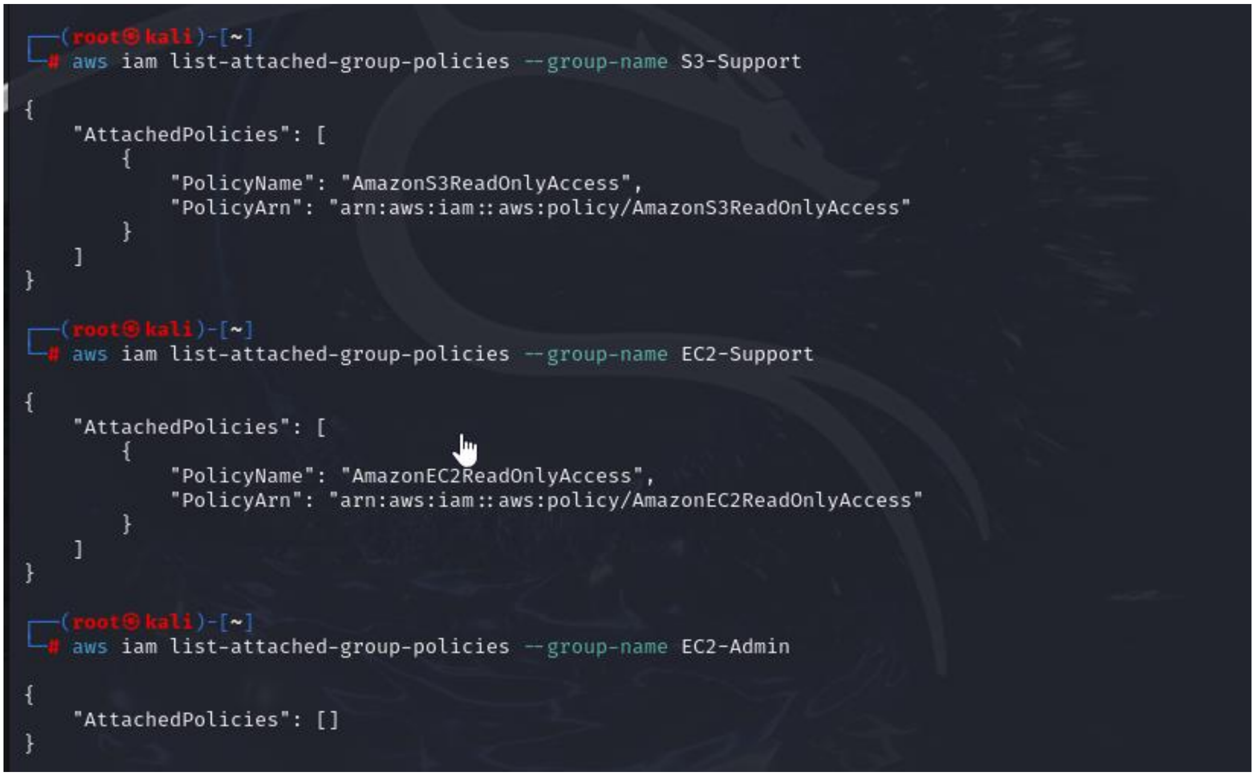


```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name S3-Support

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA2CTFHBEV7R2X36ALH",
        "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}

┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Support

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}

┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Admin

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA2CTFHBEVWF7N6KMVY",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```

3. Task 2: Inspect IAM Policies

Step 1: List Attached Policies for a Group

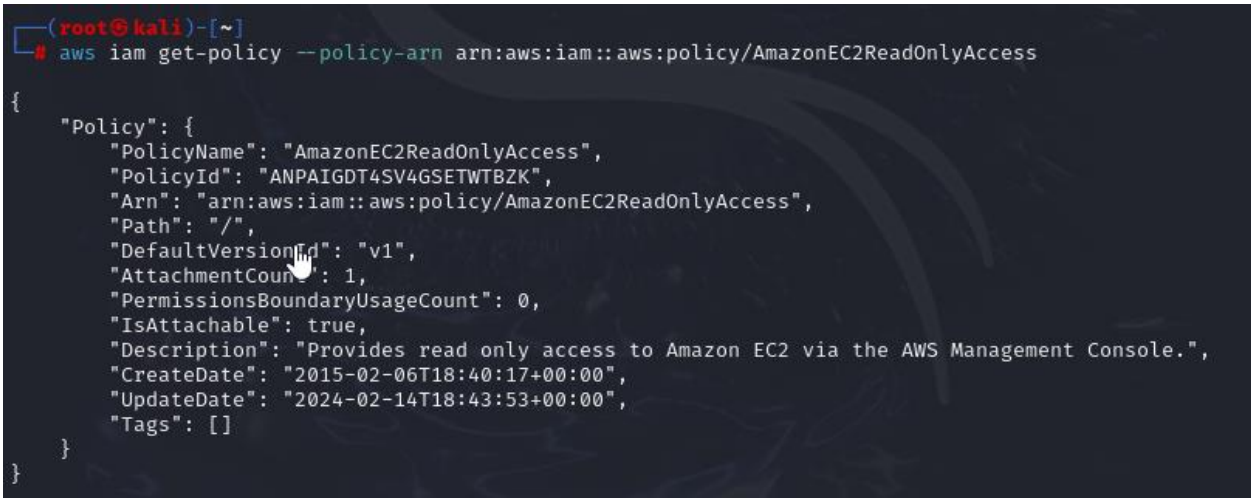
This command lists all policies attached to a specific group.



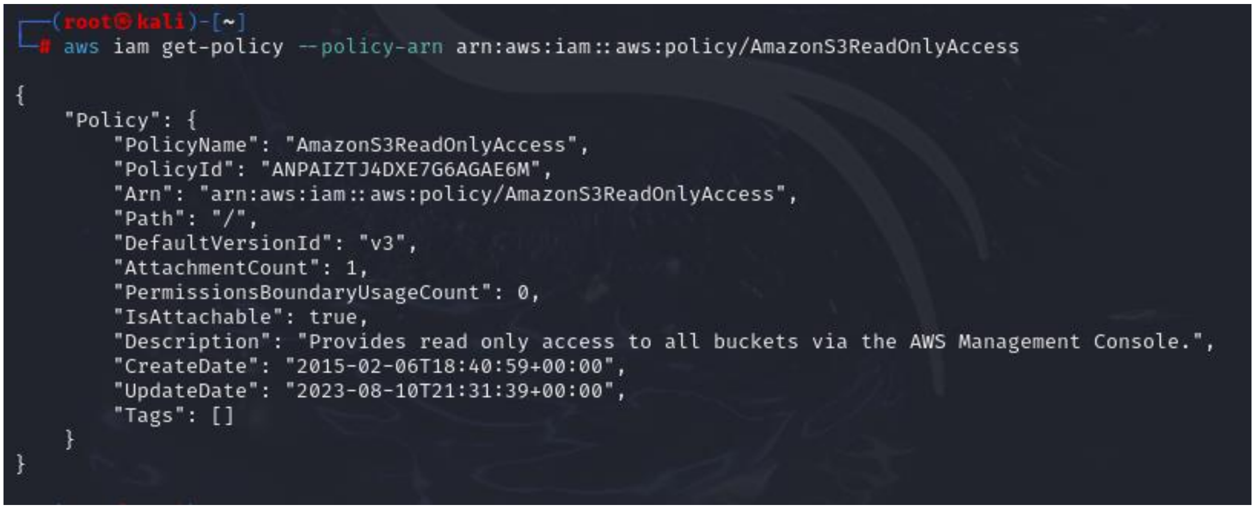
```
┌──(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name S3-Support

{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        }
    ]
}

┌──(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name EC2-Support

{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}

┌──(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name EC2-Admin

{
    "AttachedPolicies": []
}
```

Step 2: View Policy Details

To view the details of a specific policy attached to the group, use the policy's ARN (Amazon Resource Name) from the previous command's output.



```
┌──(root㉿kali)-[~]
└─# aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

{
    "Policy": {
        "PolicyName": "AmazonEC2ReadOnlyAccess",
        "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
        "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:17+00:00",
        "UpdateDate": "2024-02-14T18:43:53+00:00",
        "Tags": []
    }
}
```



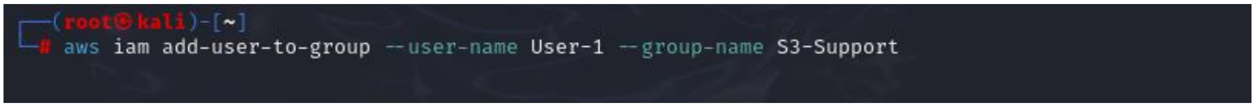
```
┌──(root㉿kali)-[~]
└─# aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

{
    "Policy": {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v3",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to all buckets via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:59+00:00",
        "UpdateDate": "2023-08-10T21:31:39+00:00",
        "Tags": []
    }
}
```

4. Task 3: Add Users to Groups

Now, add users to specific groups according to their role requirements.

Step 1: Add User-1 to S3-Support Group

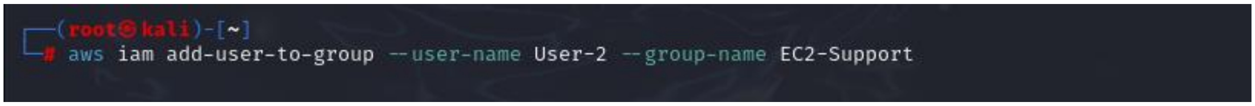
Grant User-1 read-only access to S3 by adding them to the S3-Support group.



```
┌──(root㉿kali)-[~]
└─# aws iam add-user-to-group --user-name User-1 --group-name S3-Support
```

Step 2: Add User-2 to EC2-Support Group

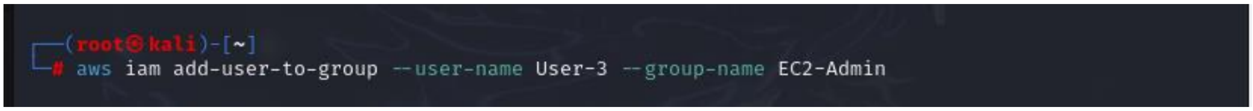
Give User-2 read-only access to EC2 resources.



```
┌──(root㉿kali)-[~]
└─# aws iam add-user-to-group --user-name User-2 --group-name EC2-Support
```

Step 3: Add User-3 to EC2-Admin Group

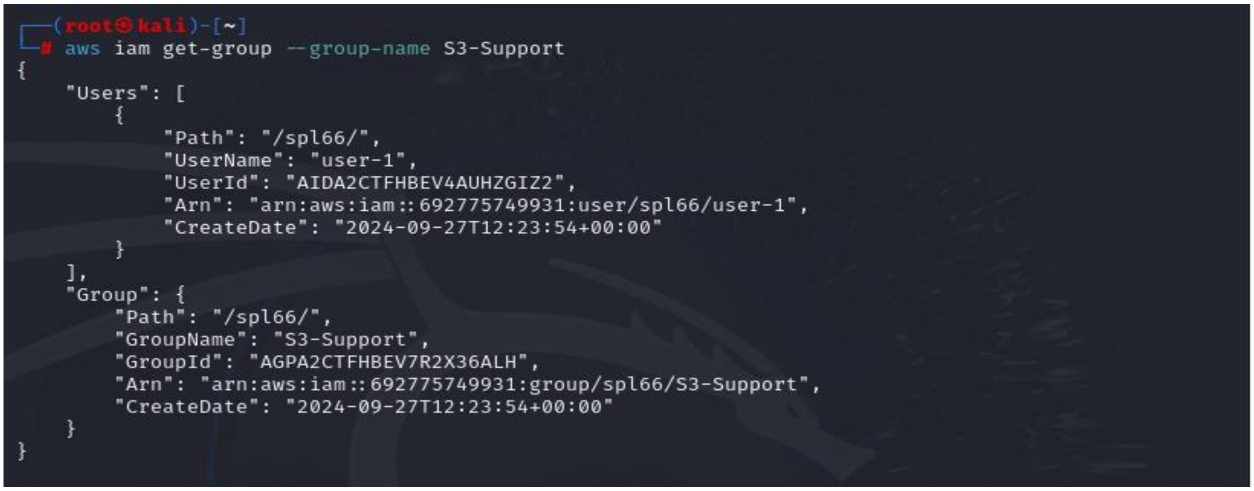
Assign User-3 permissions to view, start, and stop EC2 instances by adding them to the EC2-Admin group.



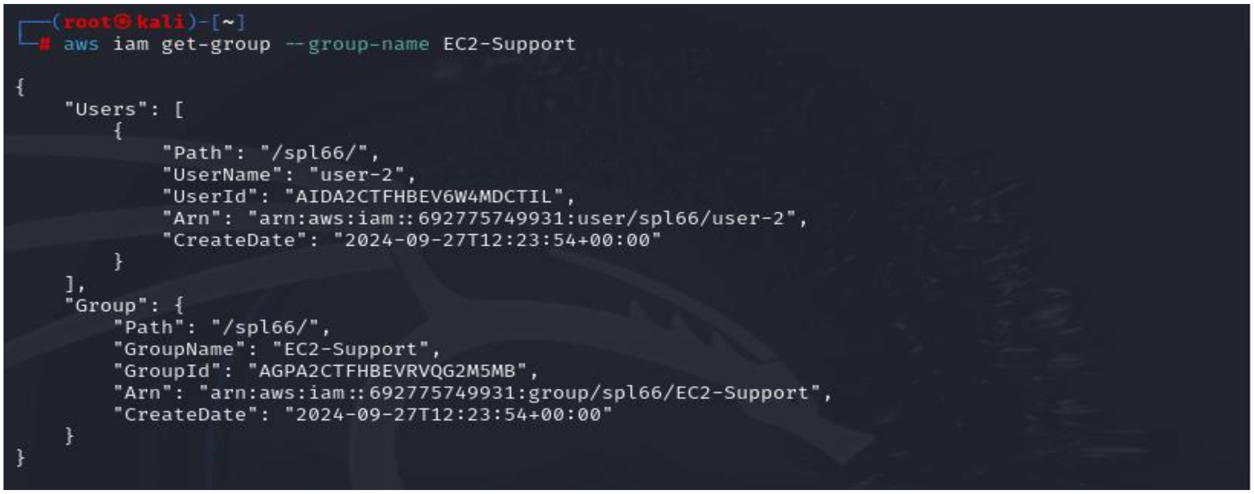
```
┌──(root㉿kali)-[~]
└─# aws iam add-user-to-group --user-name User-3 --group-name EC2-Admin
```

Step 4: Verify Users are Added to Groups

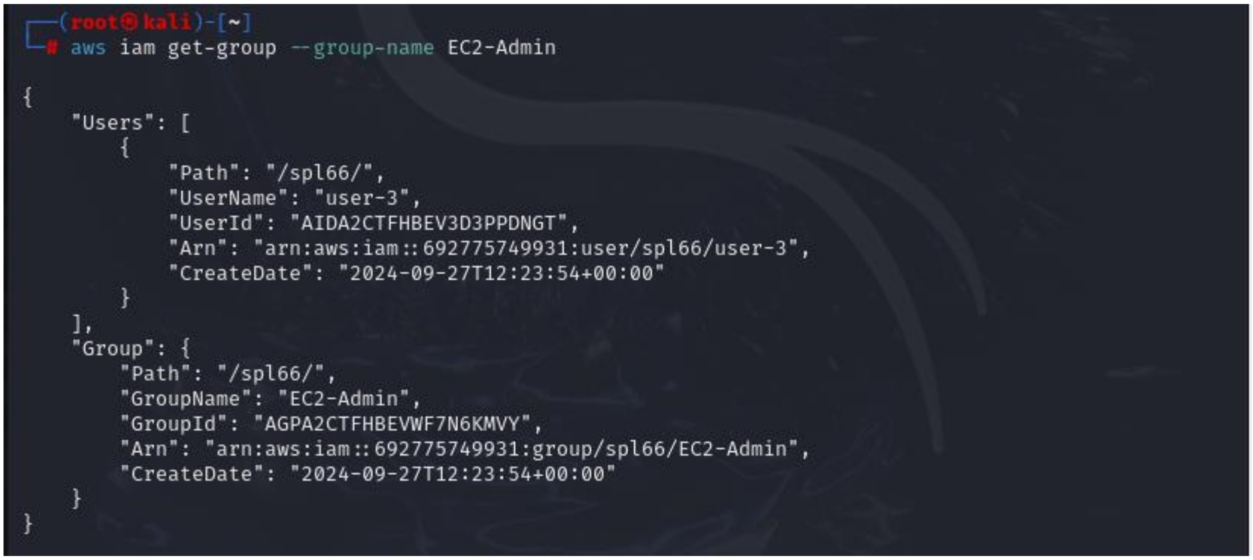
Verify that the users are properly added to the respective groups by listing users within each group.



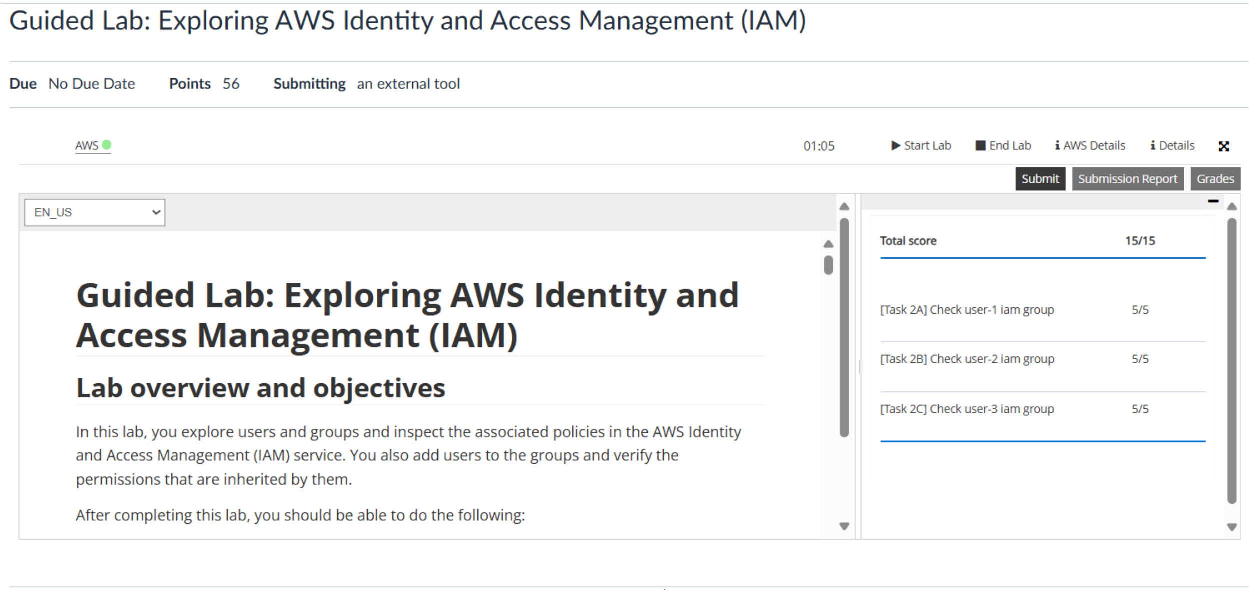
```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name S3-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA2CTFHBEV7R2X36ALH",
        "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```



```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Support

{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA2CTFHBEV6W4MDCTIL",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```



```
┌──(root㉿kali)-[~]
└─# aws iam get-group --group-name EC2-Admin

{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA2CTFHBEV3D3PPDNGT",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA2CTFHBEVWF7N6KMVY",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```



Guided Lab: Exploring AWS Identity and Access Management (IAM)

Due No Due Date **Points** 56 **Submitting** an external tool

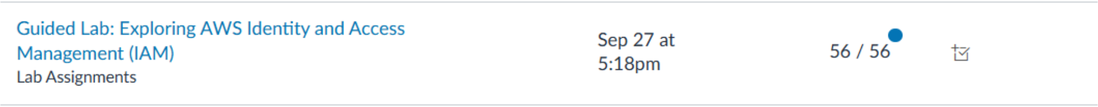
Guided Lab: Exploring AWS Identity and Access Management (IAM)

Lab overview and objectives

In this lab, you explore users and groups and inspect the associated policies in the AWS Identity and Access Management (IAM) service. You also add users to the groups and verify the permissions that are inherited by them.

After completing this lab, you should be able to do the following:

Total score	15/15
[Task 2A] Check user-1 iam group	5/5
[Task 2B] Check user-2 iam group	5/5
[Task 2C] Check user-3 iam group	5/5



Guided Lab: Exploring AWS Identity and Access Management (IAM) Lab Assignments	Sep 27 at 5:18pm	56 / 56