AWS re:Start

LAB

Introduction to IAM

WEEK 4

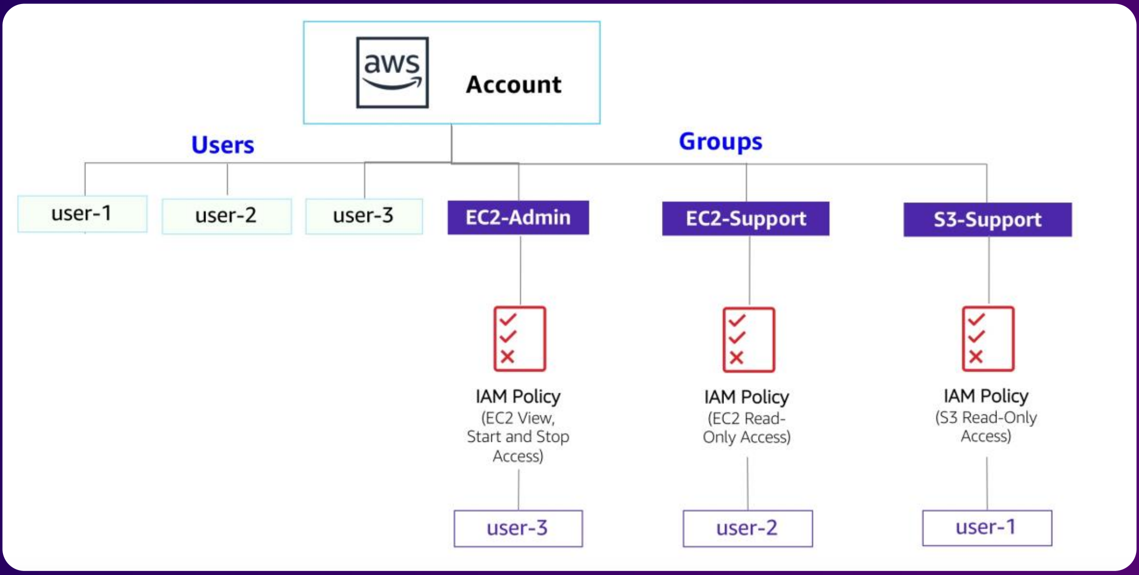
aws re/start

Overview

In many business environments, access involves a single login to a computer or a network of computer systems that provides the user access to all resources on the network. This access includes rights to personal and shared folders on a network server, company intranets, printers, and other network resources and devices. Unauthorized users can quickly exploit these same resources if the access control and associated authentication procedures are not set up properly.

In this lab, you will explore users, user groups, and policies in the AWS Identity and Access Management (IAM) service.

Here is diagram of the current environment with the listed IAM users and IAM groups

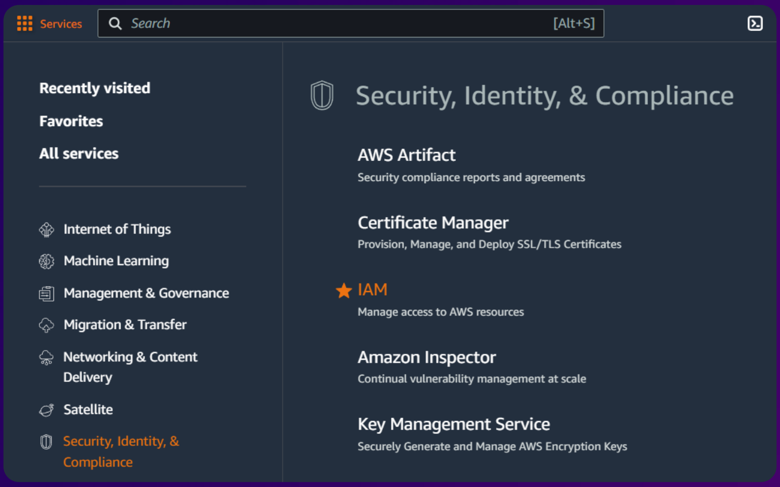


Task 1

Create an account password policy

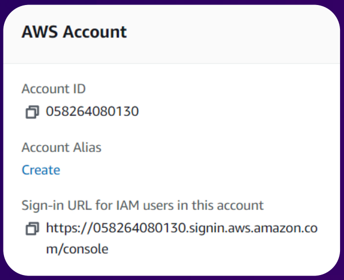
Step 1: Access the IAM service

Open the AWS Management Console, and select IAM.


Services
Search
[Alt+S]
Recently visited
Favorites
All services
Internet of Things
Machine Learning
Management & Governance
Migration & Transfer
Networking & Content Delivery
Satellite
Security, Identity, & Compliance
Security, Identity, & Compliance
AWS Artifact
Security compliance reports and agreements
Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates
IAM
Manage access to AWS resources
Amazon Inspector
Continual vulnerability management at scale
Key Management Service
Securely Generate and Manage AWS Encryption Keys

Step 2: Review the IAM Dashboard

Review the AWS Account details and the IAM resources.

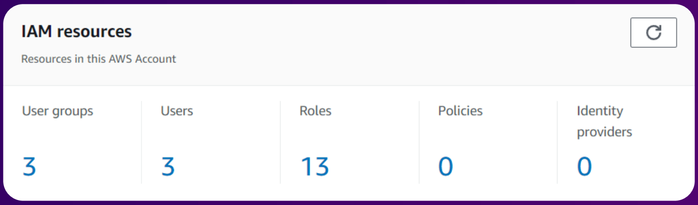


AWS Account

Account ID
058264080130

Account Alias
Create

Sign-in URL for IAM users in this account
https://058264080130.signin.aws.amazon.com/console



IAM resources

Resources in this AWS Account

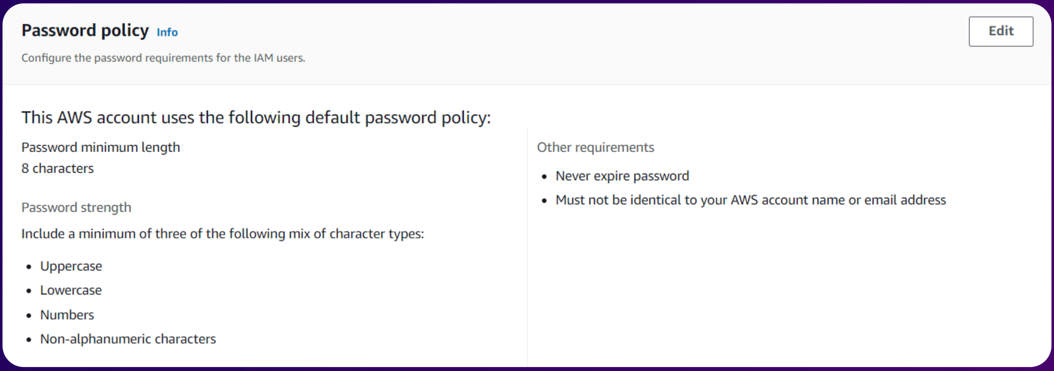
User groups	Users	Roles	Policies	Identity providers
3	3	13	0	0

Task 1

Create an account password policy

Step 3: Review the password policy

Navigate to the **Account settings** section. Here you can see the default password policy that is currently in effect. Select Edit.



Password policy Info

Configure the password requirements for the IAM users.

This AWS account uses the following default password policy:

Password minimum length
8 characters

Password strength

Include a minimum of three of the following mix of character types:

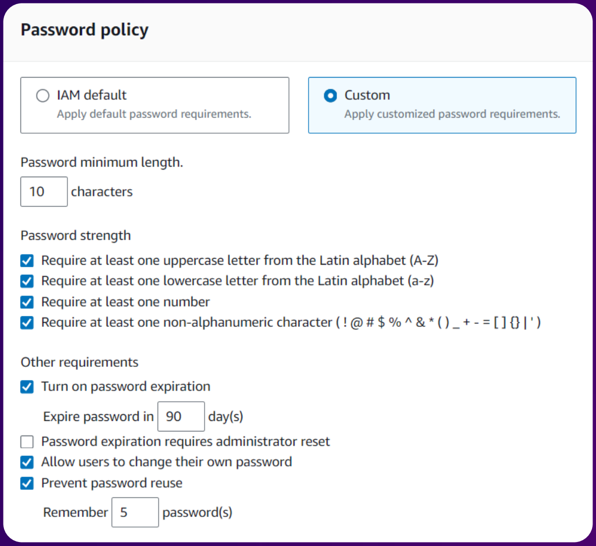
- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

Step 4: Change password policy

Create a custom password policy using the following options.



Password policy

○ IAM default
Apply default password requirements.

● Custom
Apply customized password requirements.

Password minimum length.
10 characters

Password strength

☑ Require at least one uppercase letter from the Latin alphabet (A-Z)
☑ Require at least one lowercase letter from the Latin alphabet (a-z)
☑ Require at least one number
☑ Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] {} | ')

Other requirements

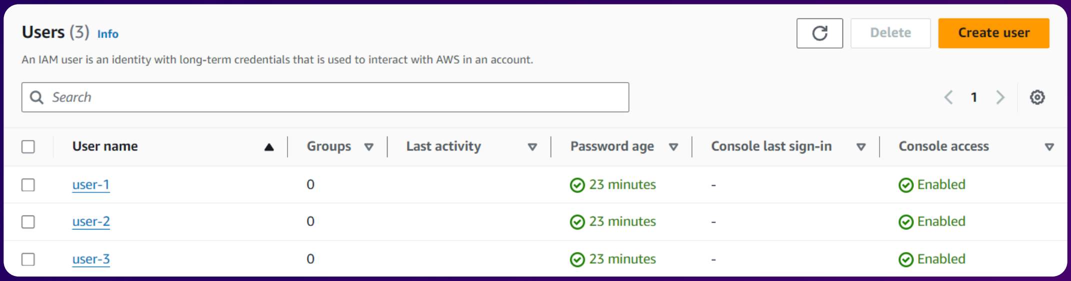
☑ Turn on password expiration
Expire password in 90 day(s)
☐ Password expiration requires administrator reset
☑ Allow users to change their own password
☑ Prevent password reuse
Remember 5 password(s)

Task 2

Explore users and user groups

Step 1: Review Users

Navigate to the **Users** section. You'll find three users listed.



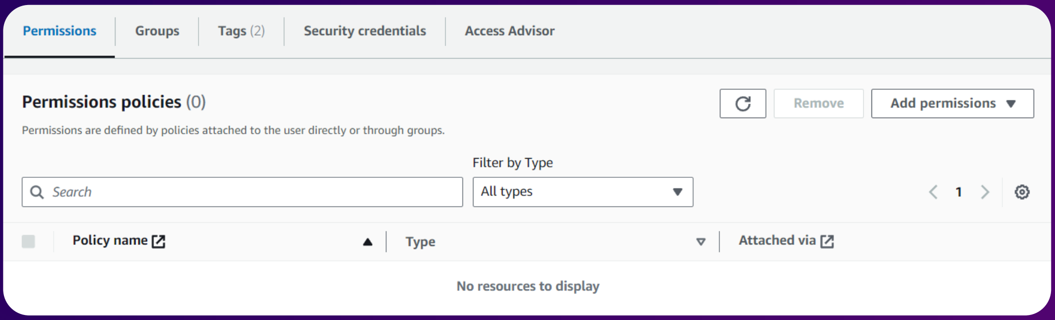
Users (3)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Groups	Last activity	Password age	Console last sign-in	Console access
□	user-1	0		✓ 23 minutes	-	✓ Enabled
□	user-2	0		✓ 23 minutes	-	✓ Enabled
□	user-3	0		✓ 23 minutes	-	✓ Enabled

Step 2: Review User permissions policies

Select user-1. Choose the **Permissions** tab. Notice that user-1 does not have any permissions.



Permissions policies (0)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

□	Policy name ▲	Type	Attached via

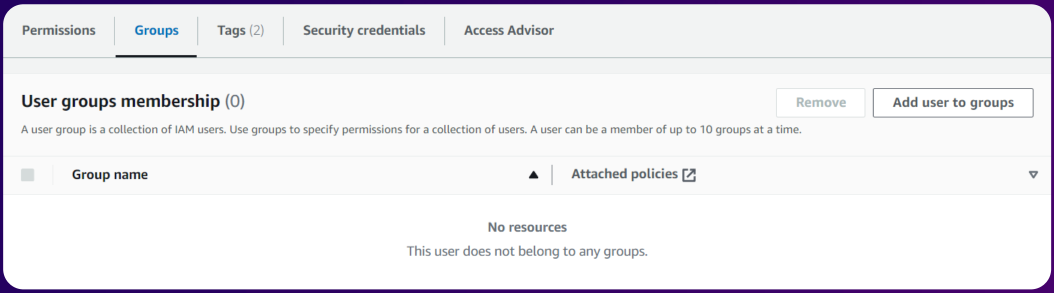
No resources to display

Task 2

Explore users and user groups

Step 3: Review User groups memberships

Choose the **Groups** tab. Notice that user-1 is also is not a member of any user groups.



User groups membership (0)

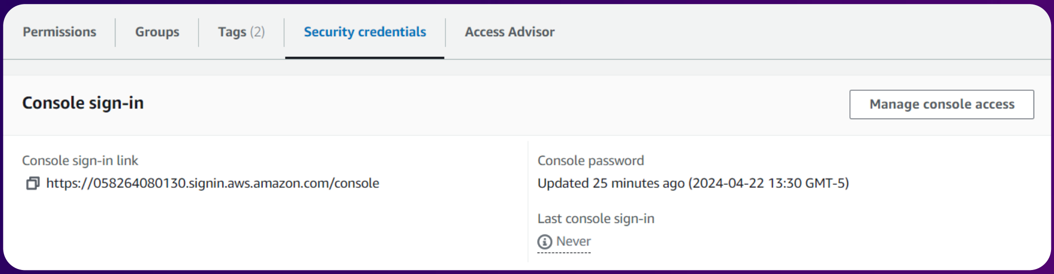
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

No resources

This user does not belong to any groups.

Step 4: Review User security credentials

Choose the **Security credentials** tab. Notice that user-1 is assigned a Console password.



Console sign-in

Console sign-in link
https://058264080130.signin.aws.amazon.com/console

Console password
Updated 25 minutes ago (2024-04-22 13:30 GMT-5)

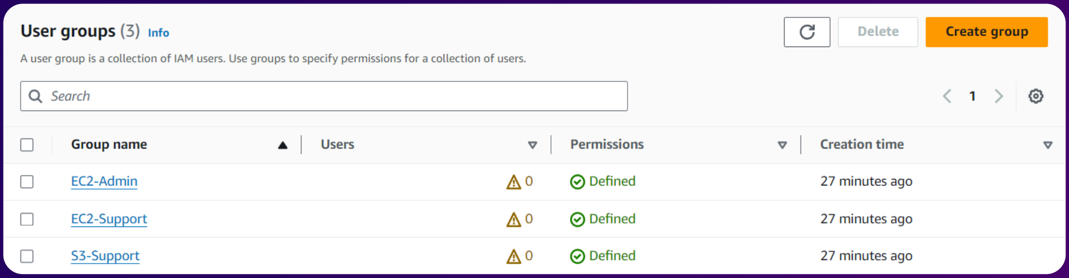
Last console sign-in
Never

Task 2

Explore users and user groups

Step 5: Review User groups

Navigate to the **Users groups** section. You'll find three user groups listed in this section.



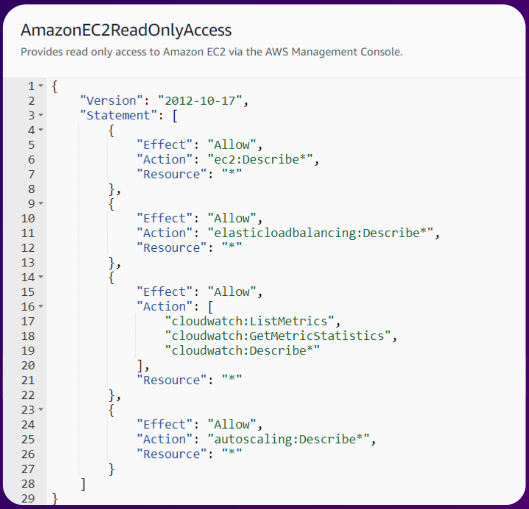
User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time
□	EC2-Admin	⚠ 0	✓ Defined	27 minutes ago
□	EC2-Support	⚠ 0	✓ Defined	27 minutes ago
□	S3-Support	⚠ 0	✓ Defined	27 minutes ago

Step 6: Review the EC2-Support policy

Choose the EC2-Support group and review its managed policy.



AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Console.

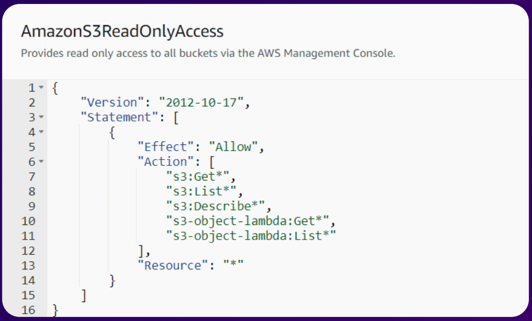
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "autoscaling:Describe*",
            "Resource": "*"
        }
    ]
}
```

Task 2

Explore users and user groups

Step 7: Review the S3-Support policy

Choose the S3-Support group and review its managed policy.



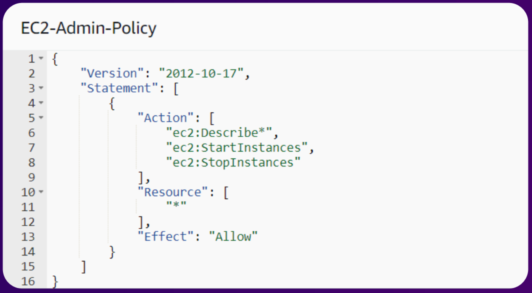
AmazonS3ReadOnlyAccess

Provides read only access to all buckets via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*",
                "s3:Describe*",
                "s3-object-lambda:Get*",
                "s3-object-lambda:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Step 8: Review the EC2-Admin policy

Choose the EC2-Admin group and review its customer inline policy.



EC2-Admin-Policy

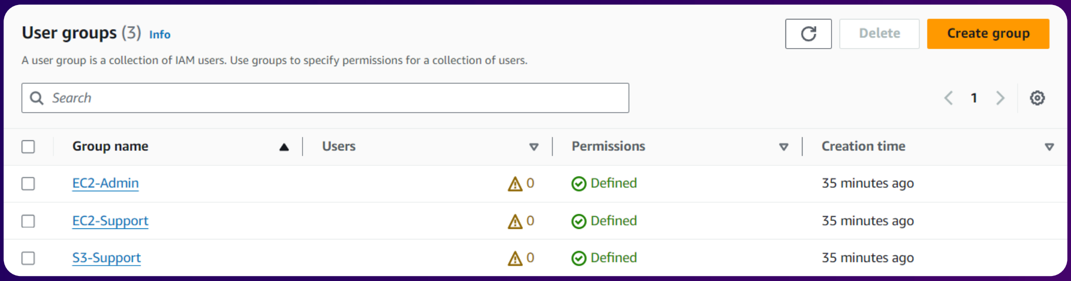
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:Describe*",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Task 3

Add users to user groups

Step 1: Review user groups members

There are currently no members in any of the user groups. Now, we will associate one user with each group.



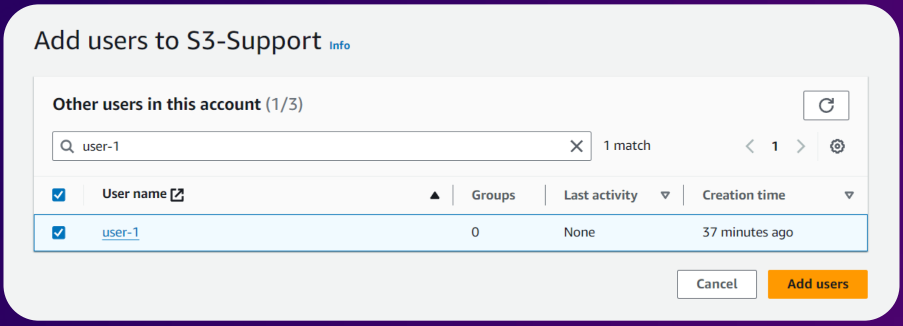
User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name ▲	Users	Permissions	Creation time
□	EC2-Admin	⚠ 0	✓ Defined	35 minutes ago
□	EC2-Support	⚠ 0	✓ Defined	35 minutes ago
□	S3-Support	⚠ 0	✓ Defined	35 minutes ago

Step 2: Add user-1 to S3-Support

Add the user-1 user to the **S3-Support** group.



Add users to S3-Support Info

Other users in this account (1/3)

user-1

1 match

☑	User name ▲	Groups	Last activity	Creation time
☑	user-1	0	None	37 minutes ago

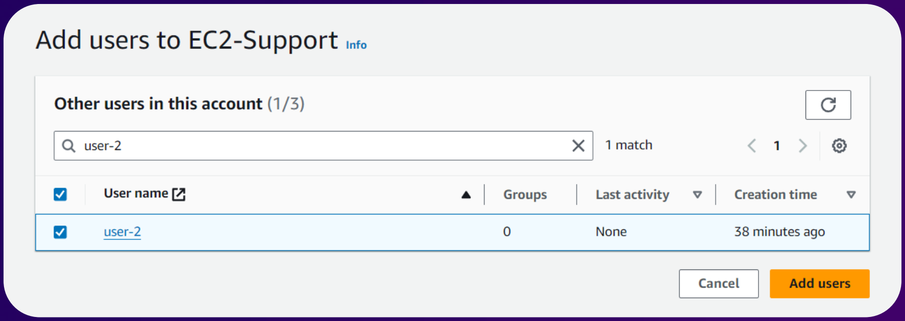
aws re/start

Task 3

Add users to user groups

Step 3: Add user-2 to EC2-Support

Add the user-2 user to the **EC2-Support** group.



Add users to EC2-Support Info

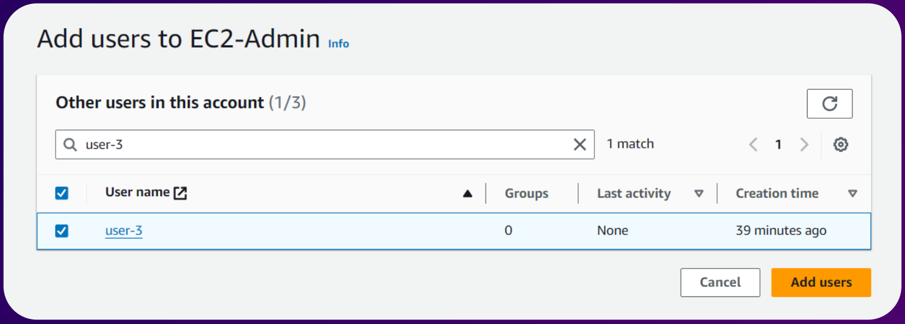
Other users in this account (1/3)

user-2 — 1 match

☑	User name	Groups	Last activity	Creation time
☑	user-2	0	None	38 minutes ago

Step 4: Add user-3 to EC2-Admin

Add the user-3 user to the **EC2-Admin** group.



Add users to EC2-Admin Info

Other users in this account (1/3)

user-3 — 1 match

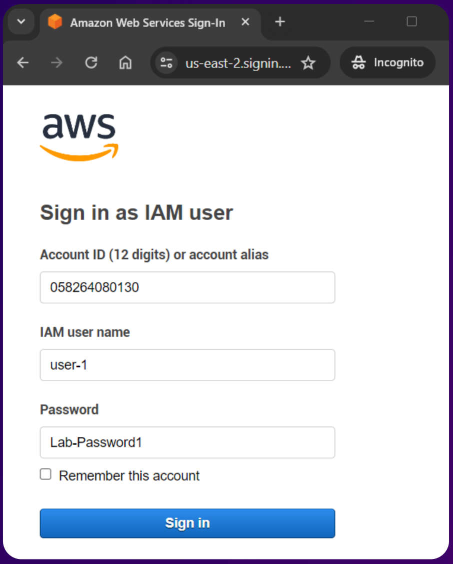
☑	User name	Groups	Last activity	Creation time
☑	user-3	0	None	39 minutes ago

Task 4

Sign in and test user permissions

Step 1: Log in as user-1

Log in as user-1 to the AWS Console using the Sign-in URL for IAM users.



Sign in as IAM user

Account ID (12 digits) or account alias: 058264080130

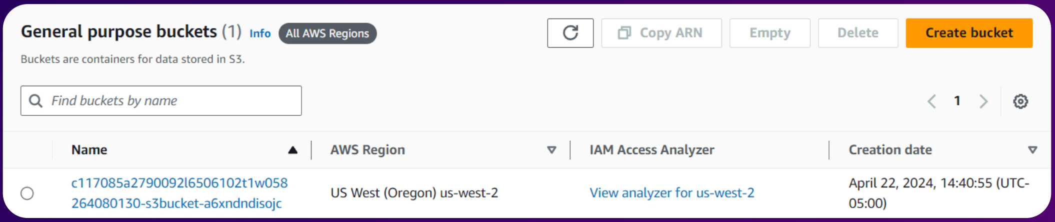
IAM user name: user-1

Password: Lab-Password1

□ Remember this account

Step 2: Review S3 buckets

Because user-1 is part of the S3-Support group in IAM, they have permission to view a list of S3 buckets.



General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	c117085a2790092l6506102t1w058264080130-s3bucket-a6xndndisojc	US West (Oregon) us-west-2	View analyzer for us-west-2	April 22, 2024, 14:40:55 (UTC-05:00)

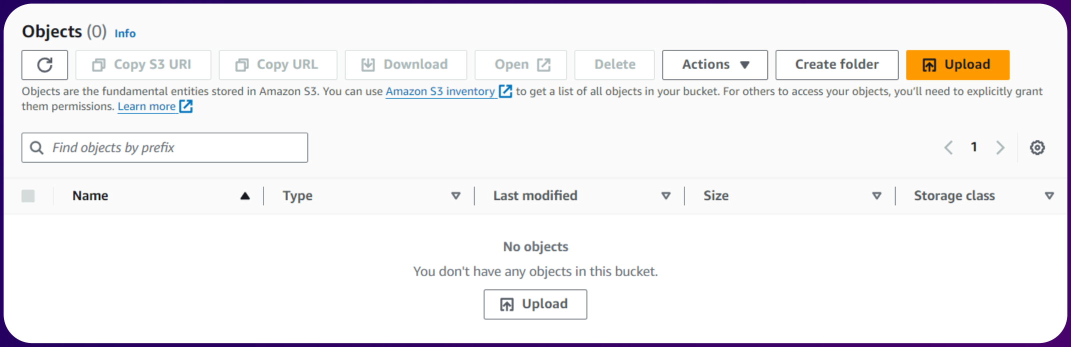
aws re/start

Task 4

Sign in and test user permissions

Step 3: Review S3 bucket contents

Because user-1 is part of the S3-Support group in IAM, they have permission to view S3 buckets contents and objects.



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

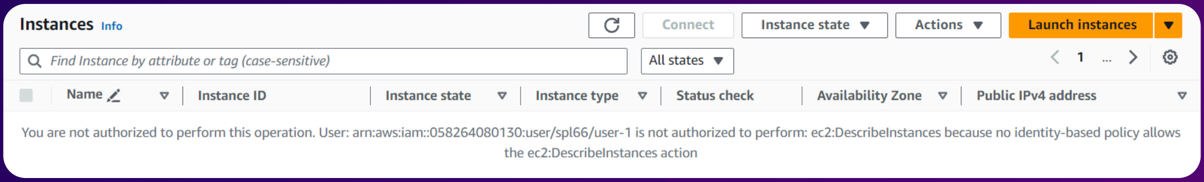
Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Step 4: Review EC2 instances

Without permissions assigned to user-1 for Amazon EC2 usage, they lack authorization to view any instances.



Name	Instance ID	Instance state	Instance type	Status check	Availability Zone	Public IPv4 address

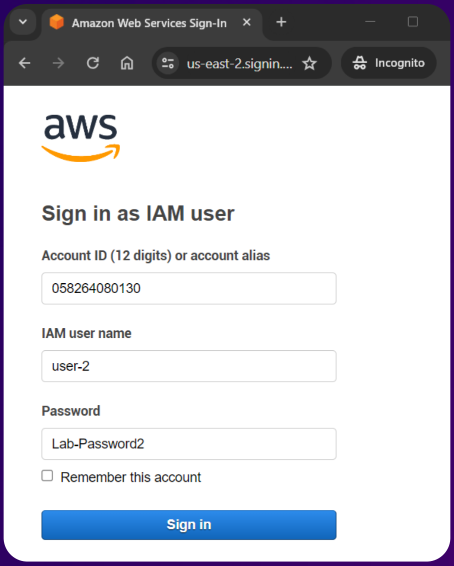
You are not authorized to perform this operation. User: arn:aws:iam::058264080130:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

Task 4

Sign in and test user permissions

Step 5: Log in as user-2

Sign out of user-1 and log in to the AWS Console as user-2.



Sign in as IAM user

Account ID (12 digits) or account alias

058264080130

IAM user name

user-2

Password

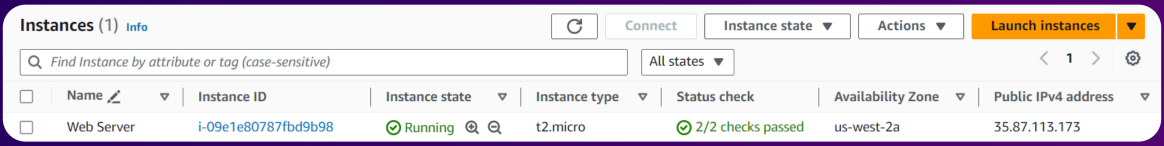
Lab-Password2

□ Remember this account

Sign in

Step 6: Review EC2 instances

You are now able to see an EC2 instance because user-2 has read-only permissions.



□	Name	Instance ID	Instance state	Instance type	Status check	Availability Zone	Public IPv4 address
□	Web Server	i-09e1e80787fbd9b98	✓ Running	t2.micro	✓ 2/2 checks passed	us-west-2a	35.87.113.173

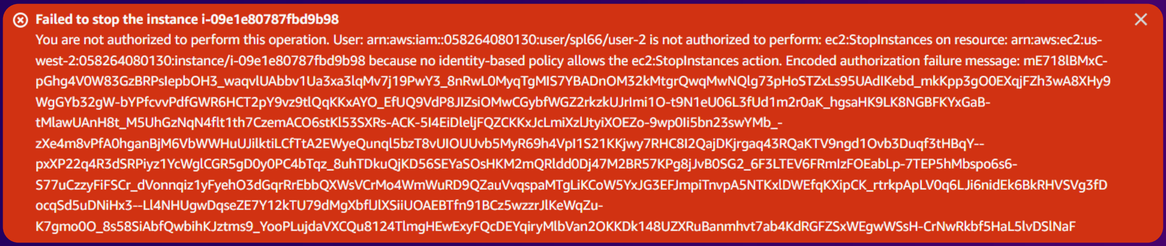
aws re/start

Task 4

Sign in and test user permissions

Step 7: Stop an instance

When attempting to stop the instance, an error occurs indicating Failed to stop the instance due to user-2 not being authorized to perform this operation.

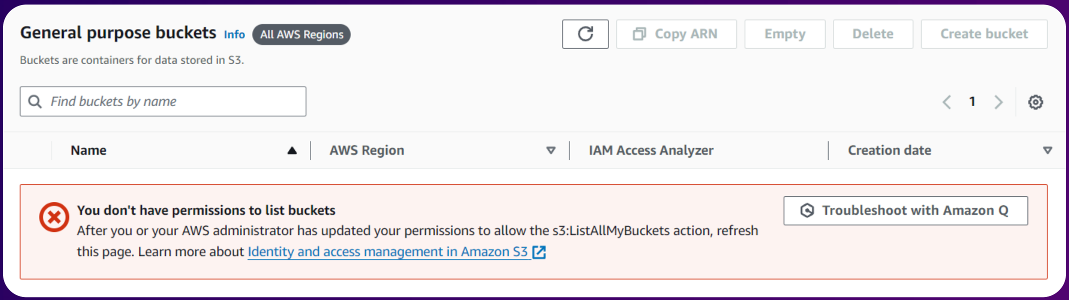


Failed to stop the instance i-09e1e80787fbd9b98

```
You are not authorized to perform this operation. User: arn:aws:iam::058264080130:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-
west-2:058264080130:instance/i-09e1e80787fbd9b98 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: mE718lBMxC-
pGhg4V0W83GzBRPslepbOH3_waqvlUAbbv1Ua3xa3lqMv7j19PwY3_8nRwL0MyqTgMIS7YBADnOM32kMtgrQwqMwNQlg73pHoSTZxLs95UAdIKebd_mkKpp3gO0EXqjFZh3wA8XHy9
WgGYb32gW-bYPfcvvPdfGWR6HCT2pY9vz9tlQqKKxAYO_EfUQ9VdP8JIZsiOMwCGybfWGZ2rkzkUJrImi1O-t9N1eU06L3fUd1m2r0aK_hgsaHK9LK8NGBFKYxGaB-
tMlawUAnH8t_M5UhGzNqN4flt1th7CzemACO6stKl53SXRs-ACK-5I4EiDleljFQZCKKxJcLmiXzlJtyiXOEZo-9wp0Ii5bn23swYMb_-
zXe4m8vPfA0hganBjM6VbWWHuUJilktiLCfTtA2EWyeQunql5bzT8vUIOUUvb5MyR69h4VpI1S21KKjwy7RHC8I2QajDKjrgaq43RQaKTV9ngd1Ovb3Duqf3tHBqY--
pxXP22q4R3dSRPiyz1YcWglCGR5gD0y0PC4bTqz_8uhTDkuQjKD56SEYaSOsHKM2mQRldd0Dj47M2BR57KPg8jJvB0SG2_6F3LTEV6FRmIzFOEabLp-7TEP5hMbspo6s6-
S77uCzzyFiFSCr_dVonnqiz1yFyehO3dGqrRrEbbQXWsVCrMo4WmWuRD9QZauVvqspaMTgLiKCoW5YxJG3EFJmpiTnvpA5NTKxlDWEfqKXipCK_rtrkpApLV0q6LJi6nidEk6BkRHVSVg3fD
ocqSd5uDNiHx3--Ll4NHUgwDqseZE7Y12kTU79dMgXbfUlXSiiUOAEBTfn91BCz5wzzrJlKeWqZu-
K7gmo0O_8s58SiAbfQwbihKJztms9_YooPLujdaVXCQu8124TlmgHEwExyFQcDEYqiryMlbVan2OKKDk148UZXRuBanmhvt7ab4KdRGFZSxWEgwWSsH-CrNwRkbf5HaL5lvDSlNaF
```

Step 8: Review S3 buckets

You receive an You don't have permissions to list buckets message because user-2 does not have permission to use Amazon S3.



General purpose buckets Info All AWS Regions

Buckets are containers for data stored in S3.

You don't have permissions to list buckets

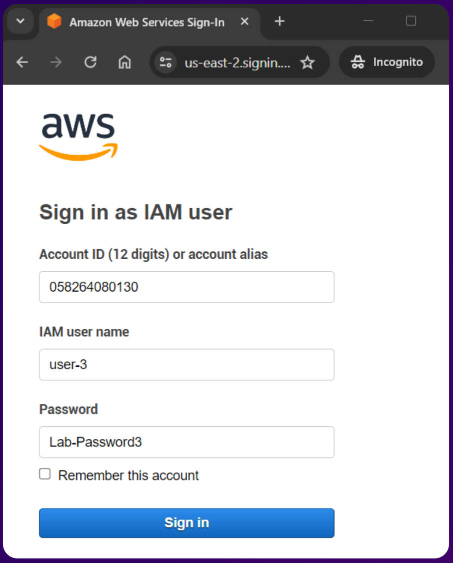
After you or your AWS administrator has updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3

Task 4

Sign in and test user permissions

Step 9: Log in as user-3

Sign out of user-2 and log in to the AWS Console as user-3.



Sign in as IAM user

Account ID (12 digits) or account alias: 058264080130

IAM user name: user-3

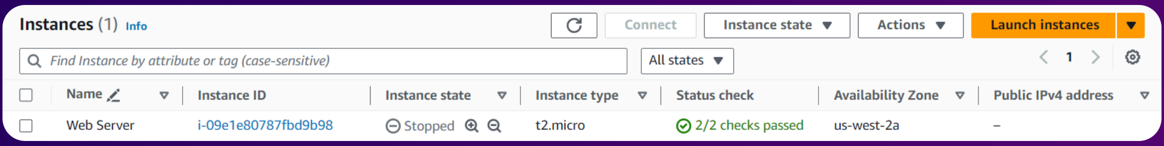
Password: Lab-Password3

☐ Remember this account

Sign in

Step 10: Stop the instance

Once logged in as user-3, you can view EC2 instances and perform the stop instance action.



☐	Name	Instance ID	Instance state	Instance type	Status check	Availability Zone	Public IPv4 address
☐	Web Server	i-09e1e80787fbd9b98	Stopped	t2.micro	2/2 checks passed	us-west-2a	–

Conclusions

IAM

Identity and Access Management (IAM) is a vital AWS service for managing user access and permissions to AWS resources securely.

IAM Users

IAM Users are individual entities with unique credentials who can interact with AWS services based on permissions assigned to them.

IAM Groups

IAM Groups are collections of IAM users with similar permissions, making it easier to manage access control at scale.

IAM Roles

IAM Roles are temporary credentials that grant specific permissions to entities like applications or services, enhancing security and reducing the need for long-term credentials.

IAM Policies

IAM Policies are JSON documents that define permissions and access control rules, allowing fine-grained control over who can do what within an AWS environment.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru

aws re/start