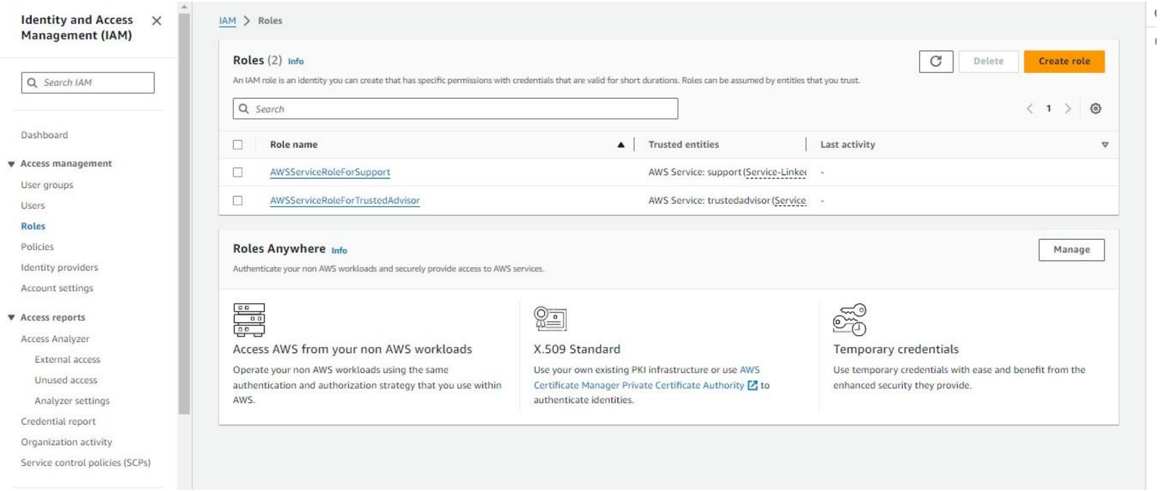
ROLE

Role is the resource of IAM service which is use to communicate between services without user we can create roles with the help of following steps:-

- Go to IAm service select the role from role option.
- Go to role select create role and select service for which we want to create role.
- Then click next and select another service which we want to give permission.
- Your role will be created.
- Go to EC2 service and create one instance (launch instances).
- Give name to instance provide image (aws Linux) & key pair.
- Your instance will be ready.
- Select instance go to action -->security --> modify IAM role.
- Change role with our role.
- Connect the instance & run aws s3 ls and our role play that we can able to see s3 buckets. (Without user login).



An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

☐	Role name	Trusted entities	Last activity
☐	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
☐	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

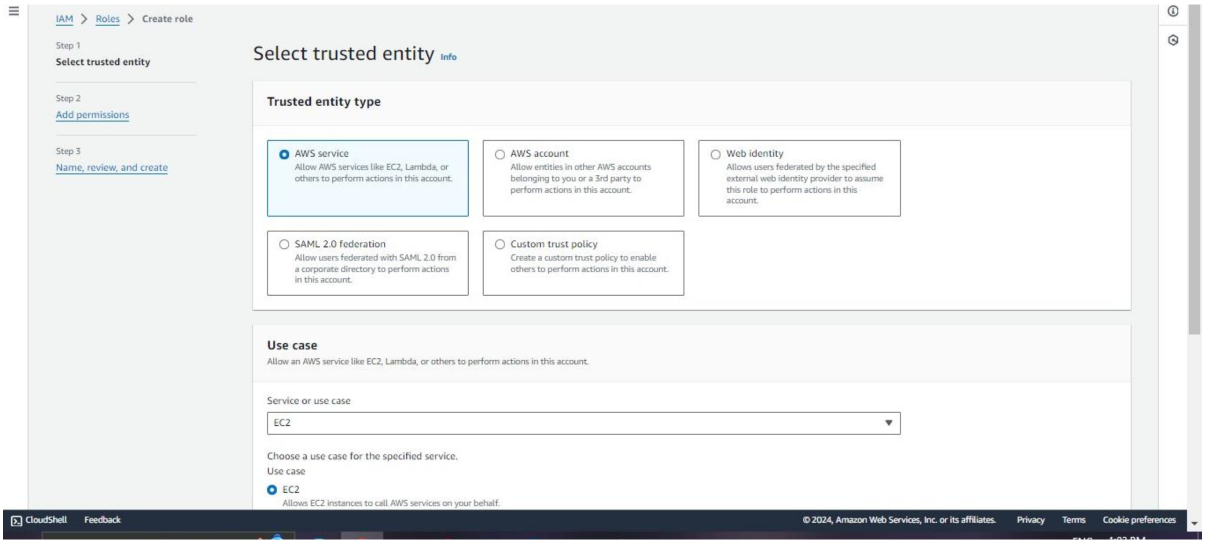
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

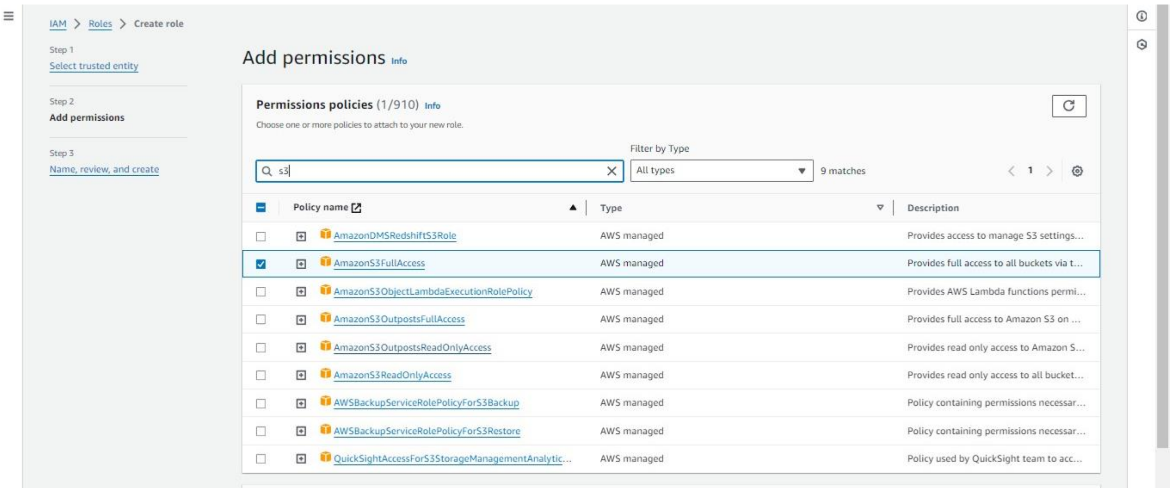
○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.
Use case
● EC2
Allows EC2 instances to call AWS services on your behalf.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

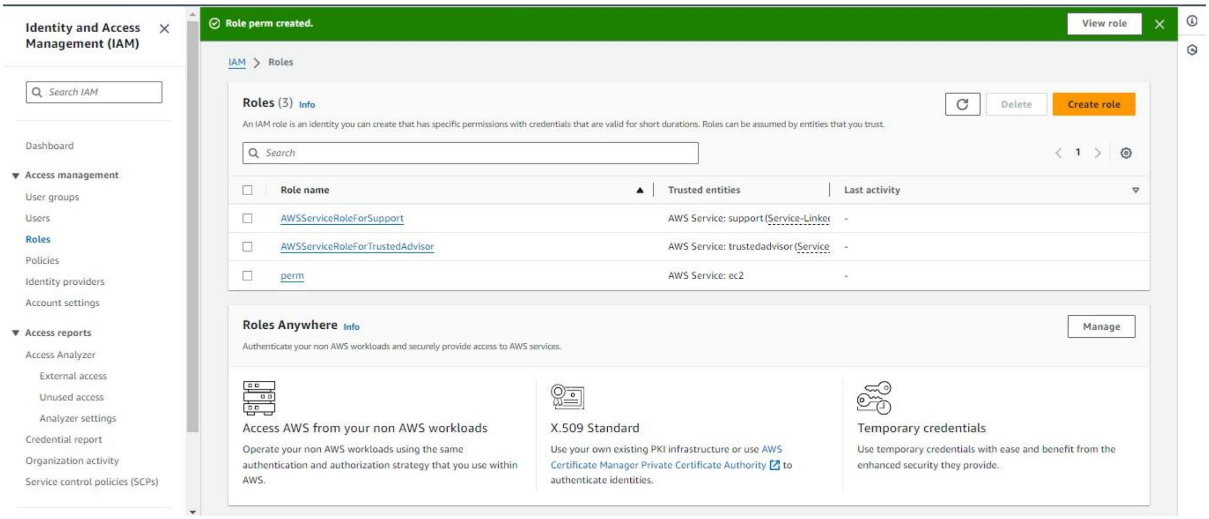
Permissions policies (1/910) Info
Choose one or more policies to attach to your new role.

s3

Filter by Type
All types

9 matches

	Policy name	Type	Description
□	AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings…
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t…
□	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions permi…
□	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on …
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S…
□	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket…
□	AWSBackupServiceRolePolicyForS3Backup	AWS managed	Policy containing permissions necessar…
□	AWSBackupServiceRolePolicyForS3Restore	AWS managed	Policy containing permissions necessar…
□	QuickSightAccessForS3StorageManagementAnalytic…	AWS managed	Policy used by QuickSight team to acc…



Role perm created.

Roles (3)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	perm	AWS Service: ec2	-

Roles Anywhere

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

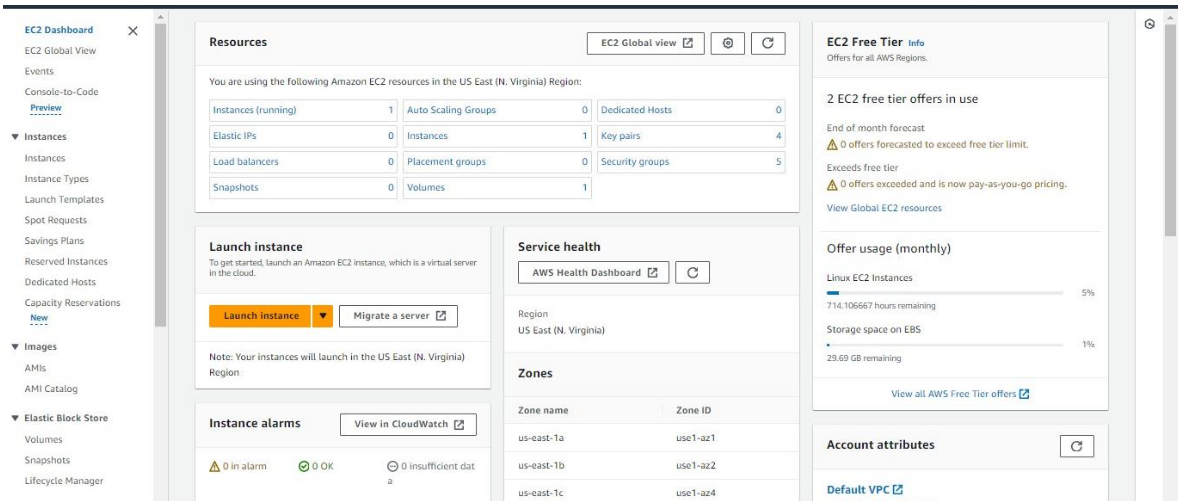
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	1	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	1	Key pairs	4
Load balancers	0	Placement groups	0	Security groups	5
Snapshots	0	Volumes	1		

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (N. Virginia) Region

Instance alarms

0 in alarm 0 OK 0 insufficient dat a

Service health

Region
US East (N. Virginia)

Zones

Zone name	Zone ID
us-east-1a	use1-az1
us-east-1b	use1-az2
us-east-1c	use1-az4

EC2 Free Tier

Offers for all AWS Regions.

2 EC2 free tier offers in use

End of month forecast
0 offers forecasted to exceed free tier limit.

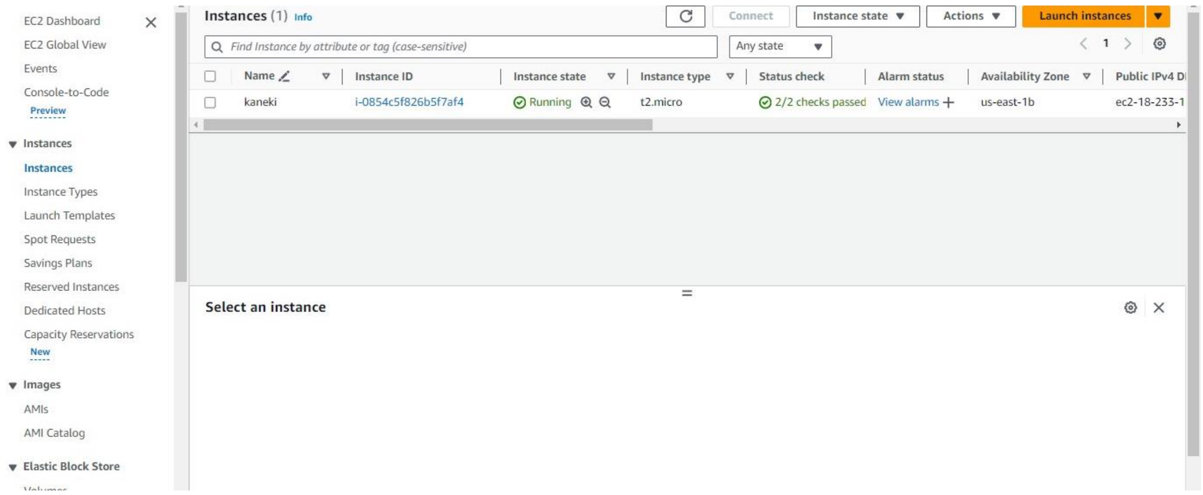
Exceeds free tier
0 offers exceeded and is now pay-as-you-go pricing.

Offer usage (monthly)

Linux EC2 Instances 5%
714.106667 hours remaining

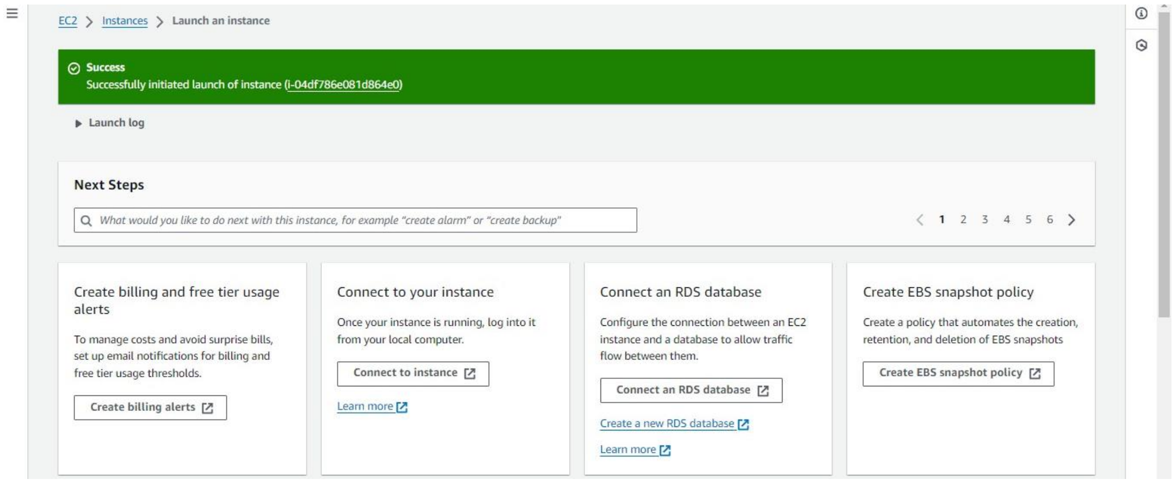
Storage space on EBS 1%
29.69 GB remaining

Account attributes



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
kaneki	i-0854c5f826b5f7af4	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-18-233-1

Select an instance


EC2 > Instances > Launch an instance
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6

Success
Successfully initiated launch of instance (i-04df786e081d864e0)

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Learn more

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

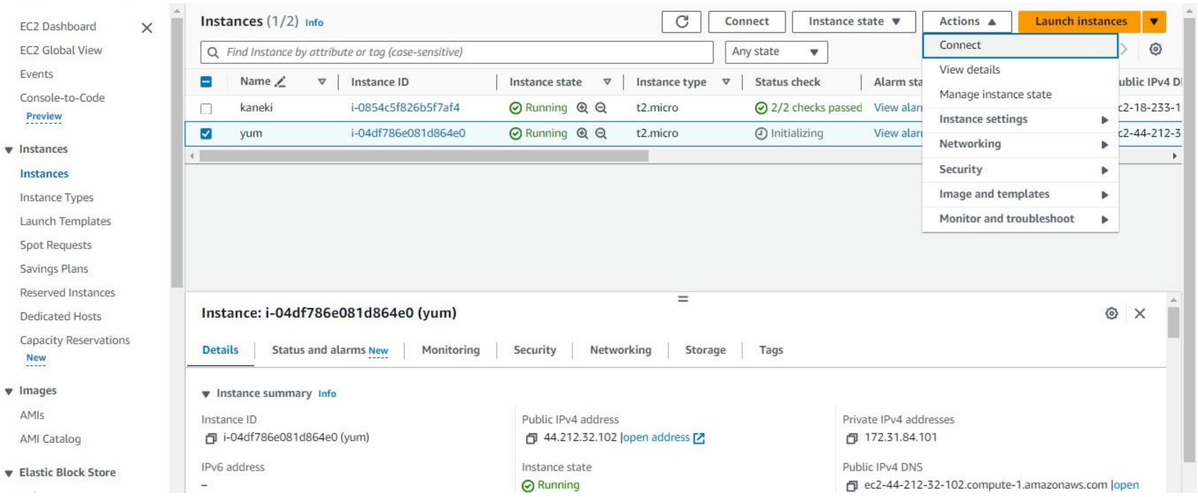
Create a new RDS database

Learn more

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Create EBS snapshot policy



	Name	Instance ID	Instance state	Instance type	Status check	Alarm sta	ublic IPv4 D
□	kaneki	i-0854c5f826b5f7af4	Running	t2.micro	2/2 checks passed	View alar	c2-18-233-1
☑	yum	i-04df786e081d864e0	Running	t2.micro	Initializing	View alar	c2-44-212-3

Instance: i-04df786e081d864e0 (yum)

Instance ID
i-04df786e081d864e0 (yum)

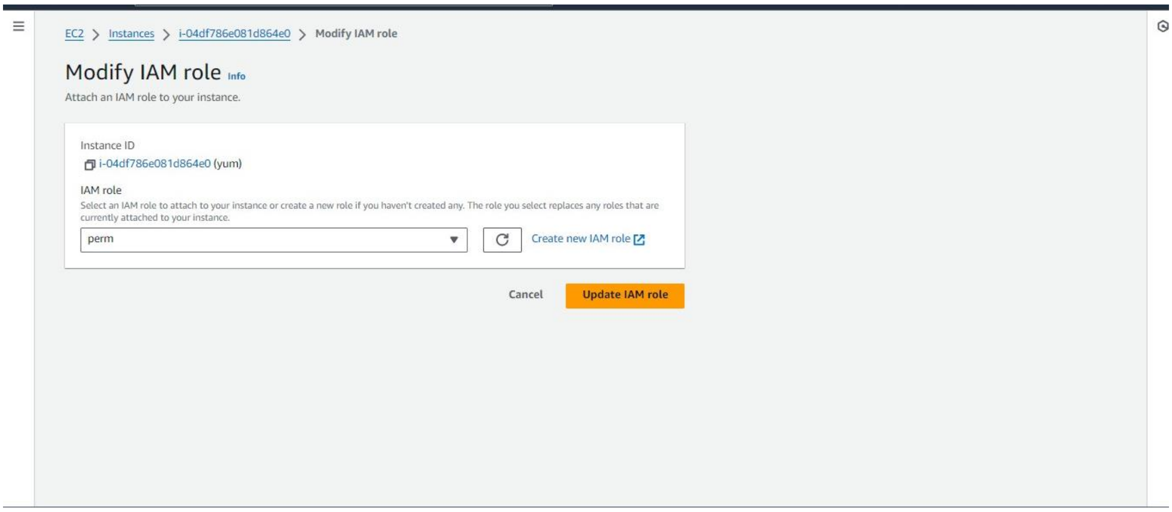
Public IPv4 address
44.212.32.102 |open address

Private IPv4 addresses
172.31.84.101

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-44-212-32-102.compute-1.amazonaws.com |open



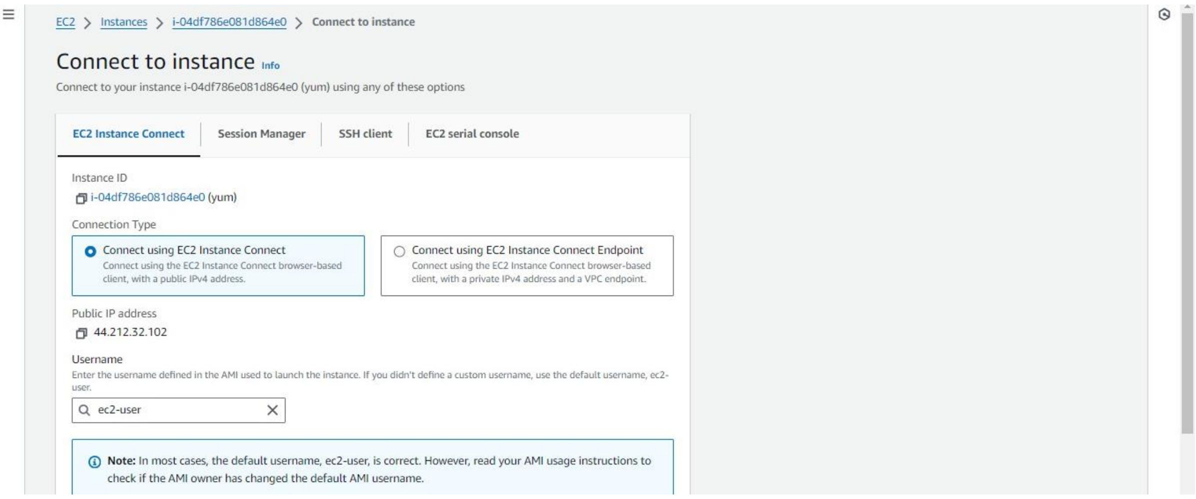
Modify IAM role Info

Attach an IAM role to your instance.

Instance ID
i-04df786e081d864e0 (yum)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

perm



EC2 > Instances > i-04df786e081d864e0 > Connect to instance

Connect to instance Info

Connect to your instance i-04df786e081d864e0 (yum) using any of these options

Instance ID

i-04df786e081d864e0 (yum)

Connection Type

● Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address

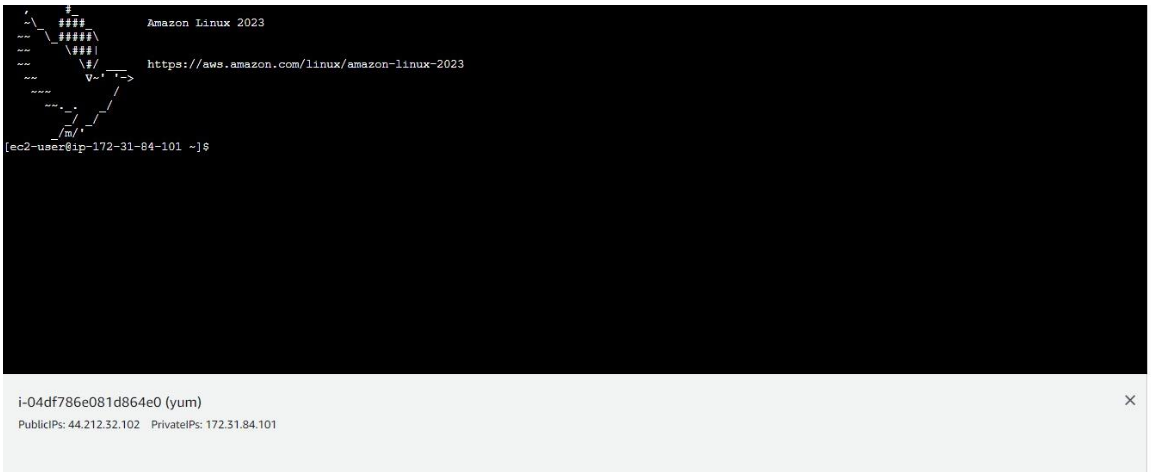
44.212.32.102

Username

Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

ec2-user

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-84-101 ~]$
```

i-04df786e081d864e0 (yum)

PublicIPs: 44.212.32.102   PrivateIPs: 172.31.84.101