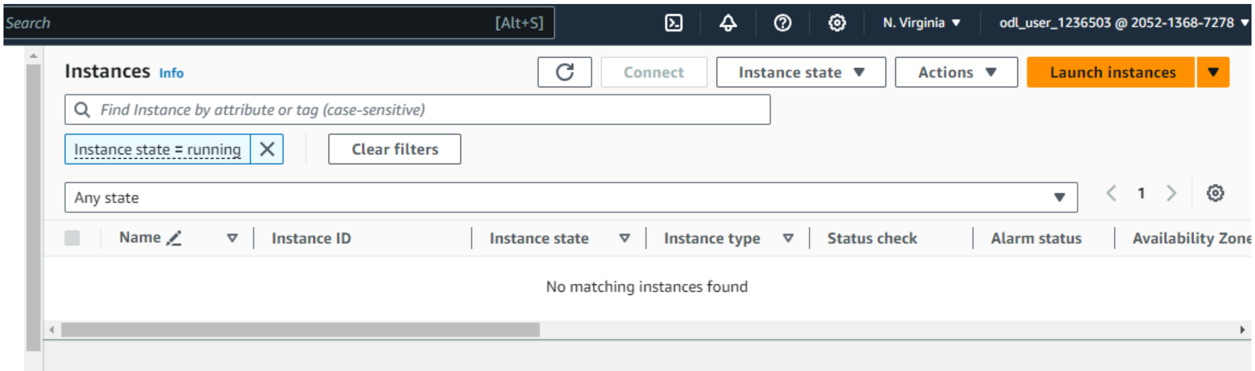
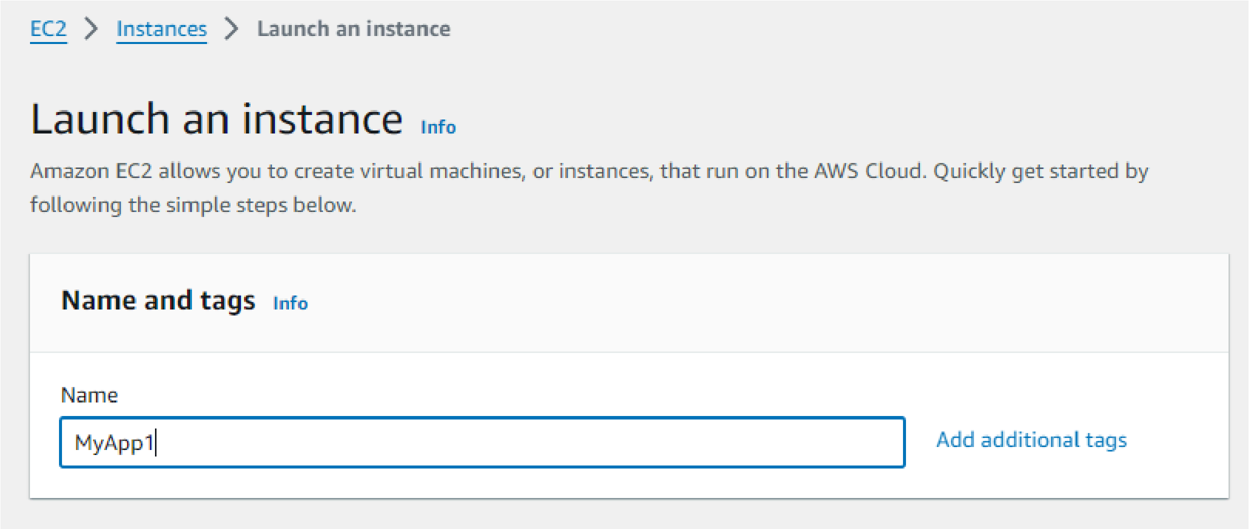
Create EC2 Instance

Go to Amzon Console and click on Instances.



No matching instances found

Click On Launch Instances.



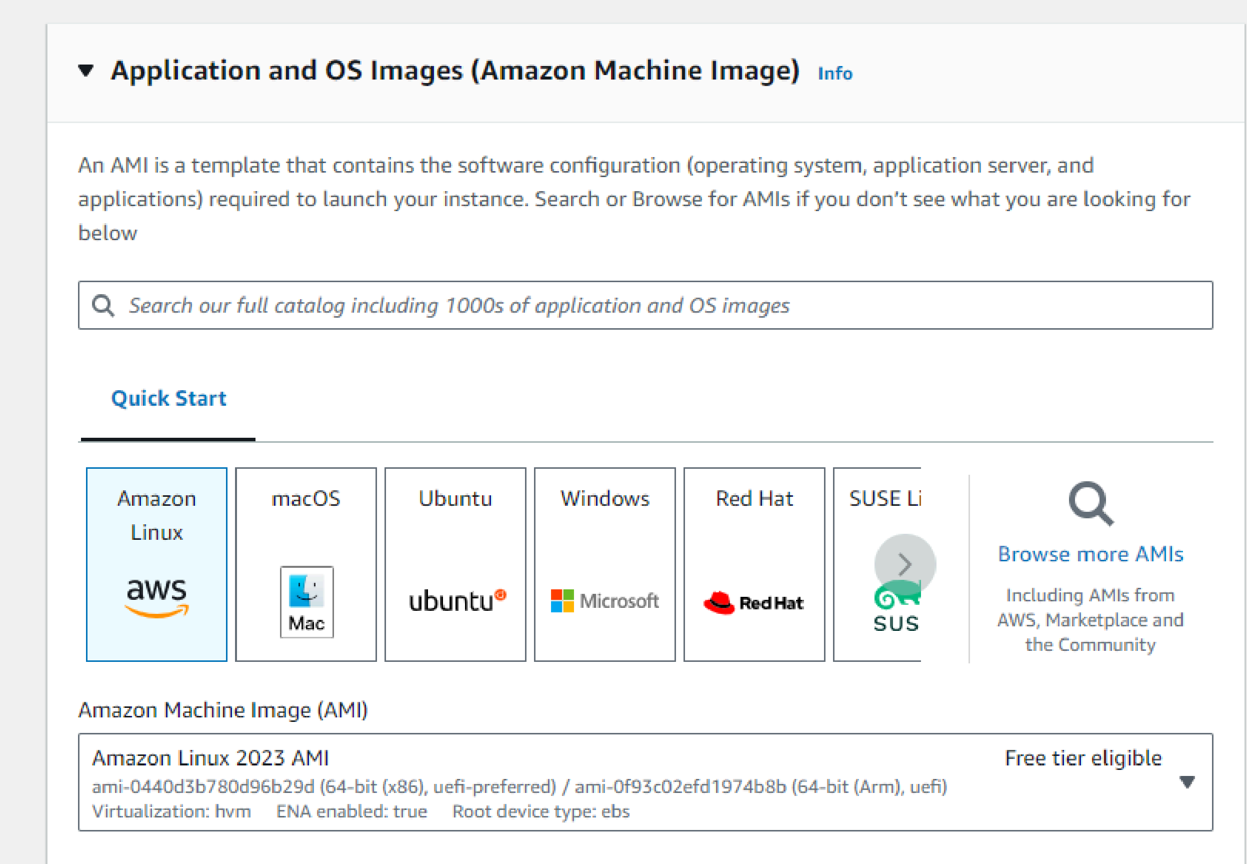
Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: MyApp1

Select Amazon Linux



▼ Application and OS Images (Amazon Machine Image) Info

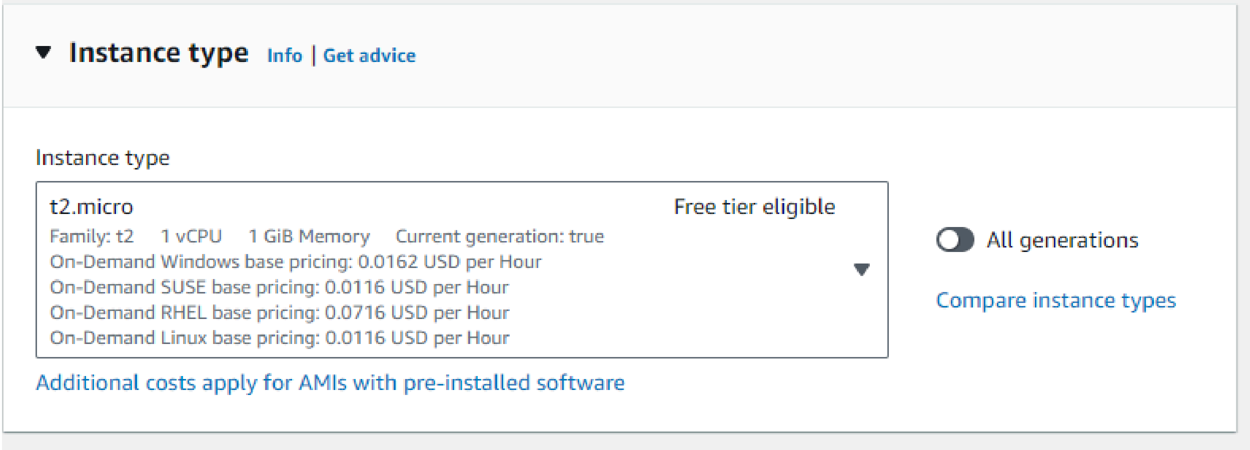
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0440d3b780d96b29d (64-bit (x86), uefi-preferred) / ami-0f93c02efd1974b8b (64-bit (Arm), uefi)
Virtualization: hvm   ENA enabled: true   Root device type: ebs

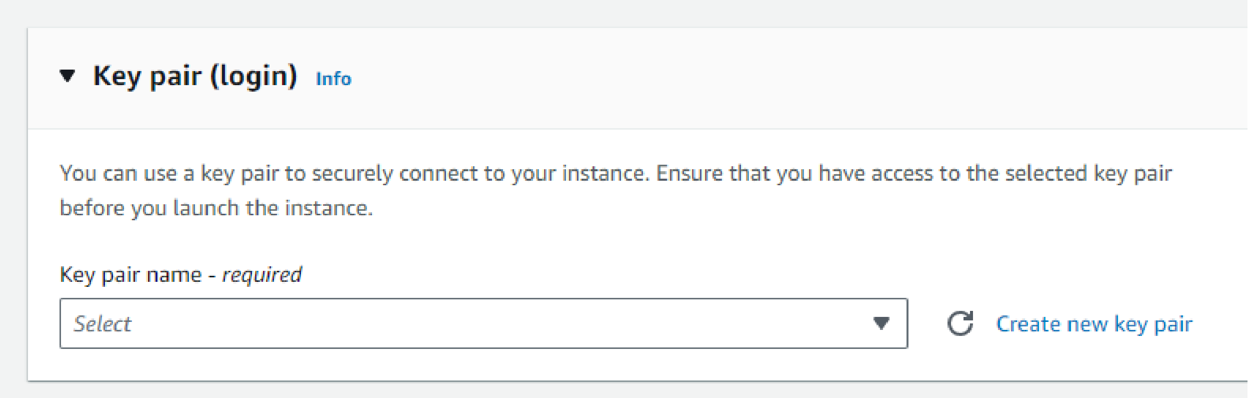
Instance Type t2.micro



▼ Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible
Family: t2   1 vCPU   1 GiB Memory   Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour



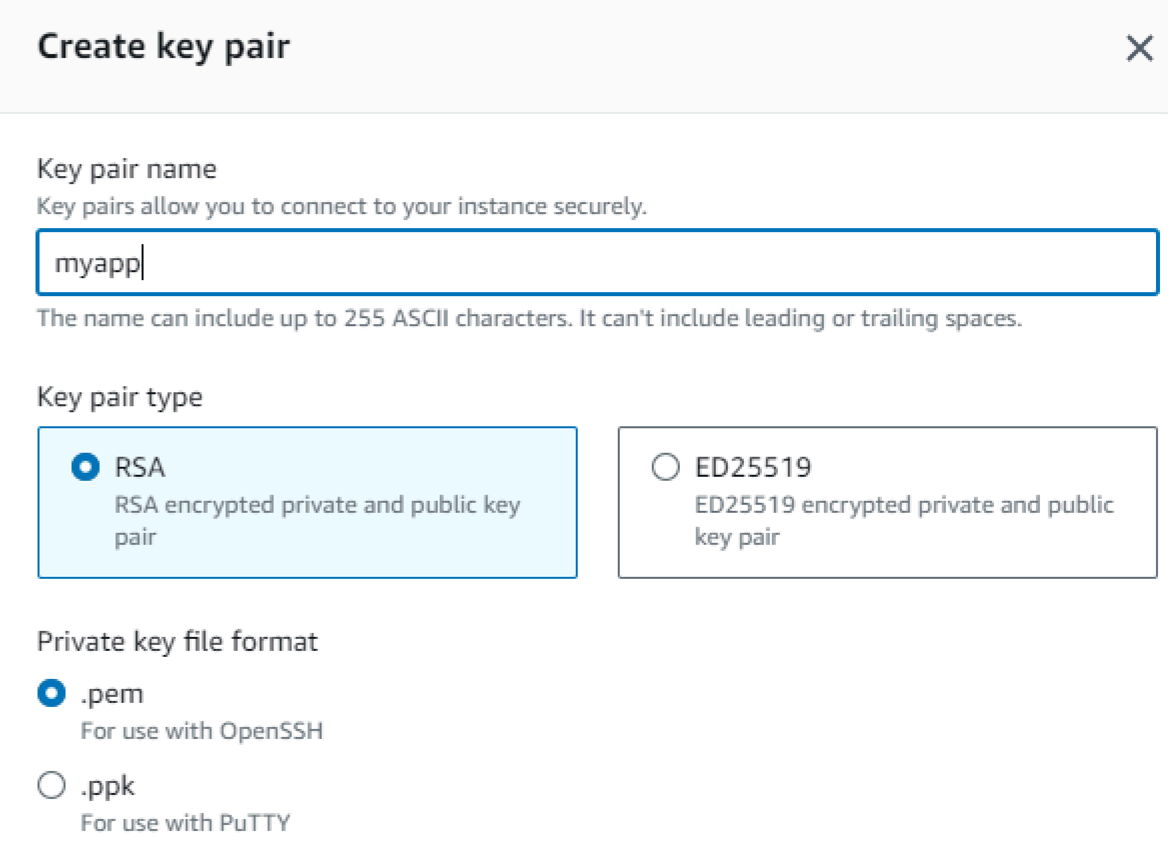
▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼ | Create new key pair

If no key pair is available click on Create New Key Pair.



Create key pair ✕

Key pair name

Key pairs allow you to connect to your instance securely.

myapp

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair

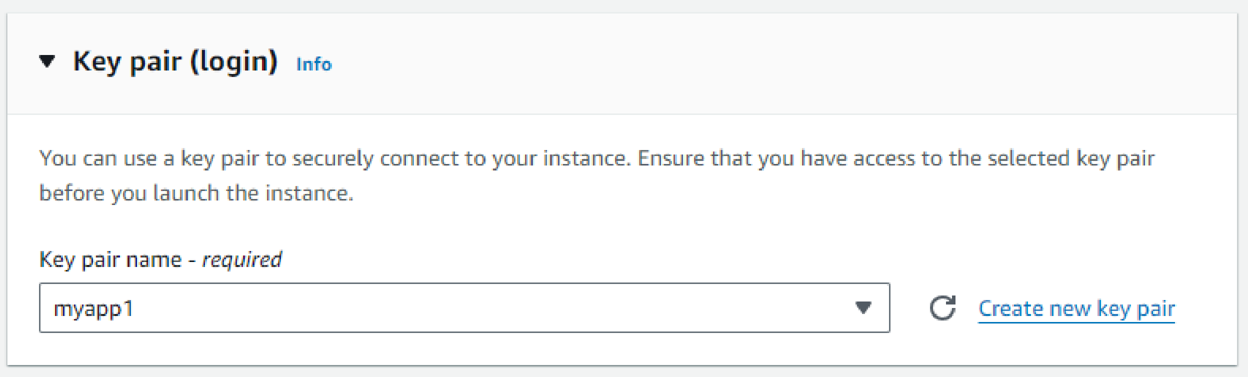
Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

Here we are selecting .pem for connect our system to this AWS instance using Open SSH.
If you want to connect using putty software then you can use .ppk generation.

When this key pair is generated then it will download this .pem file to your system. So keep it safe to connect with Instance.



▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

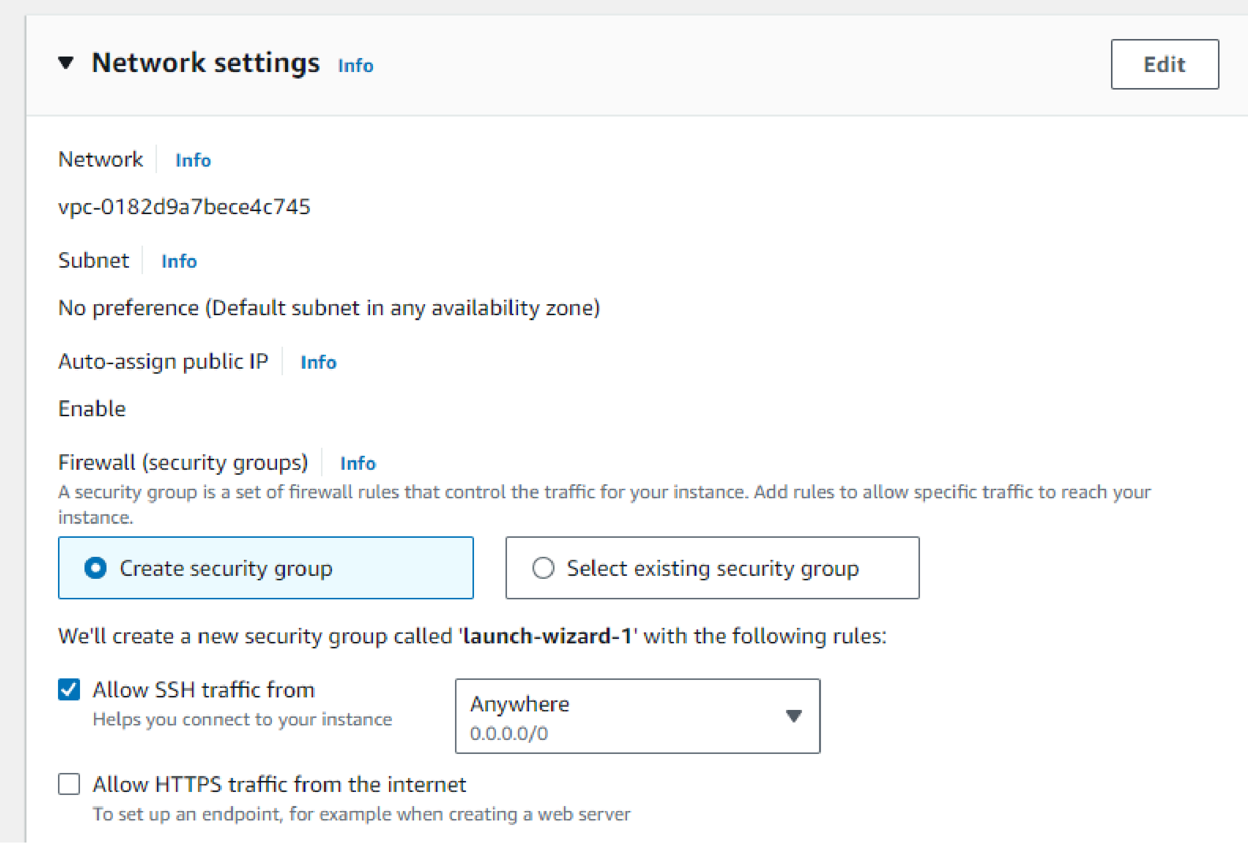
Key pair name - *required*

myapp1 ▼

Create new key pair

Select that created key value pair.

In Network settings click on Edit button



▼ Network settings Info

Edit

Network Info

vpc-0182d9a7bece4c745

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group

○ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

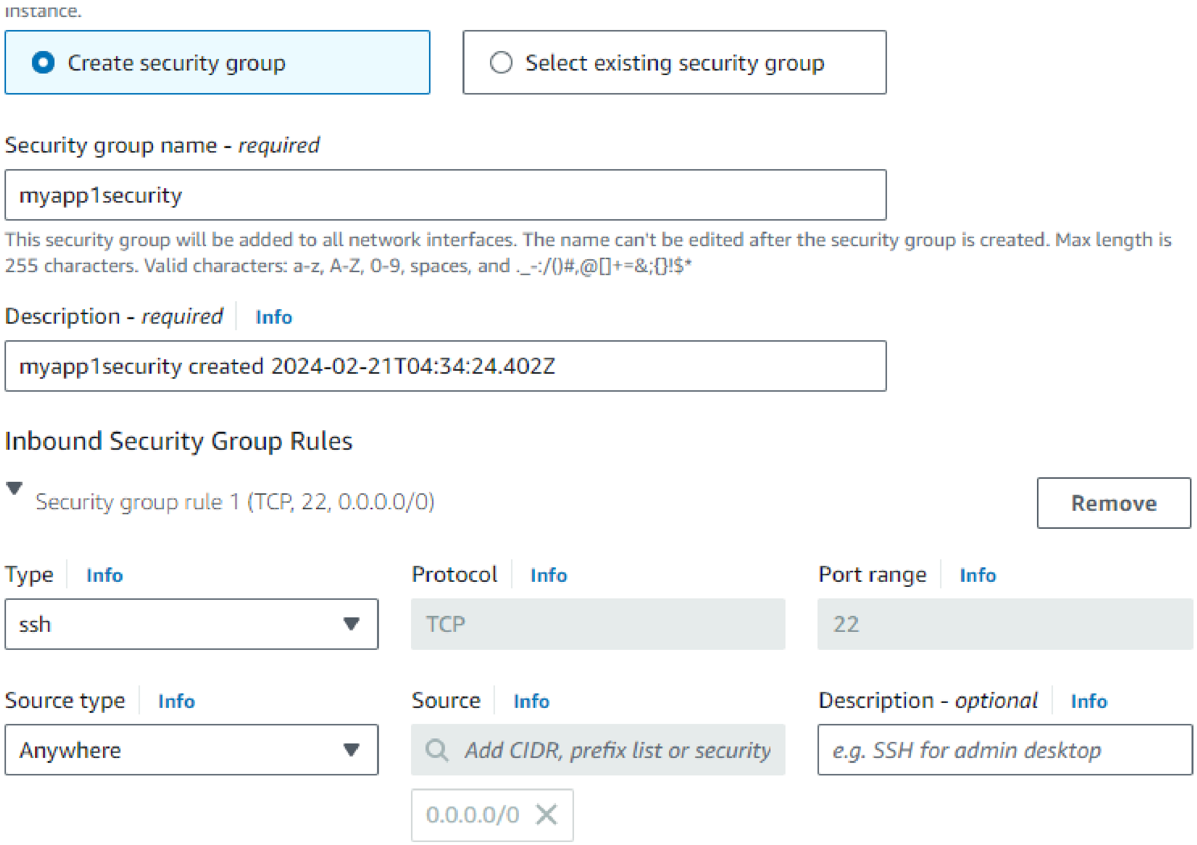
☑ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0 ▼

□ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server


instance.

● Create security group ○ Select existing security group

Security group name - *required*

myapp1security

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

myapp1security created 2024-02-21T04:34:24.402Z

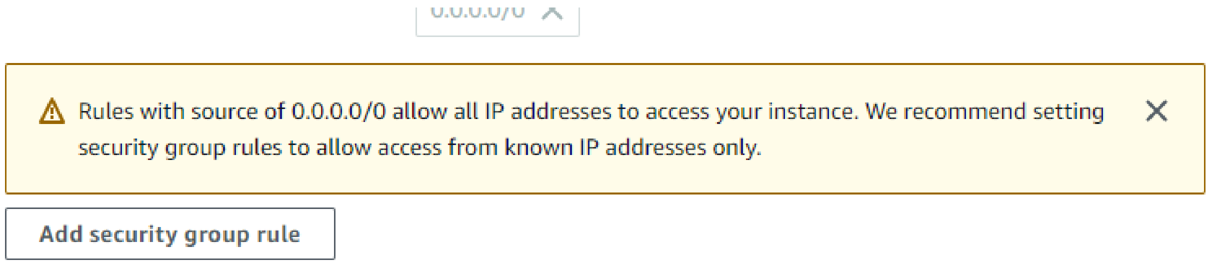
Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

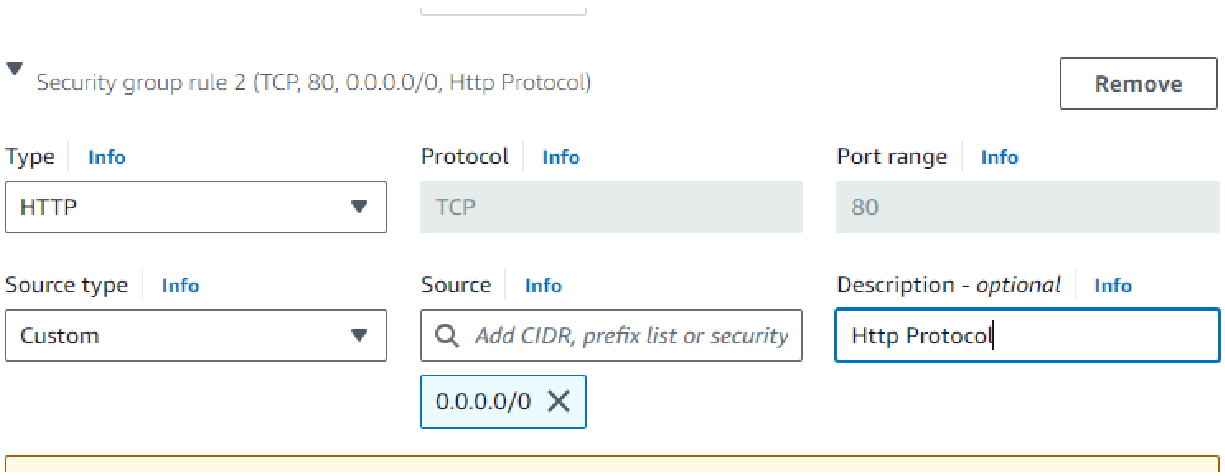
Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0 ✕	e.g. SSH for admin desktop

Change the name and description.

Don’t change anything in ssh config. Below that there is a button add new Security group click on that.


0.0.0.0/0 ✕

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕



Security group rule 2 (TCP, 80, 0.0.0.0/0, Http Protocol)

Type: HTTP

Protocol: TCP

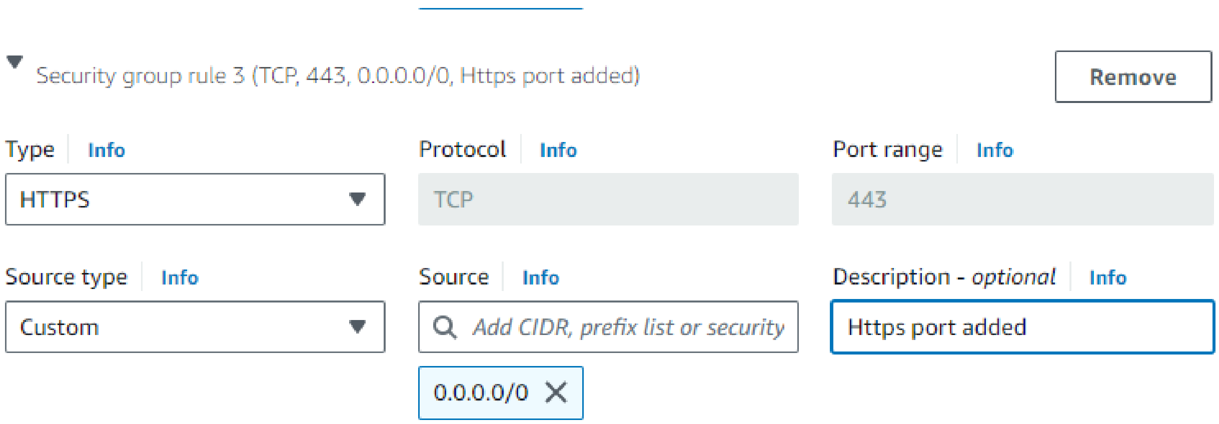
Port range: 80

Source type: Custom

Source: 0.0.0.0/0

Description - *optional*: Http Protocol

Similarly if you want to add HTTPs again click on Add New Security Groups.



Security group rule 3 (TCP, 443, 0.0.0.0/0, Https port added)

Type: HTTPS

Protocol: TCP

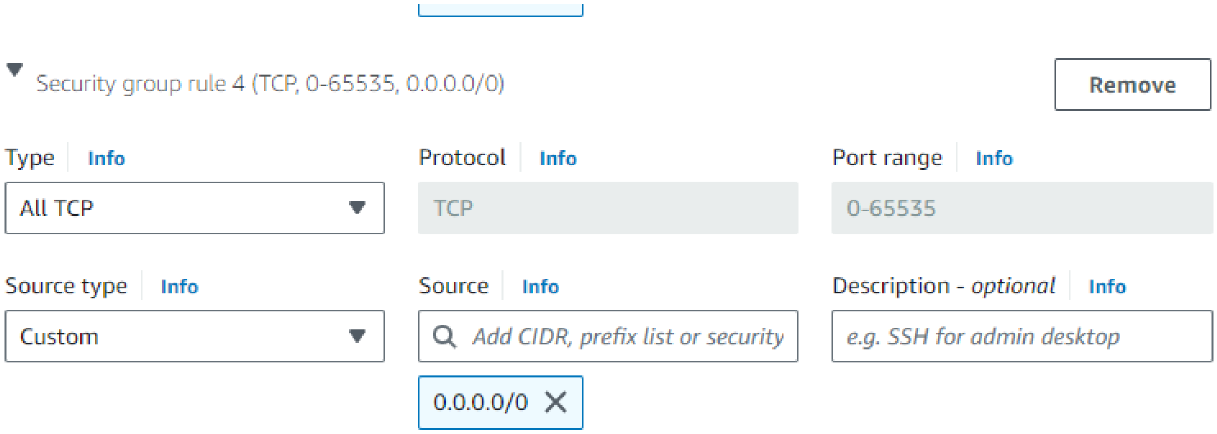
Port range: 443

Source type: Custom

Source: 0.0.0.0/0

Description - *optional*: Https port added

Configure All TCP



Security group rule 4 (TCP, 0-65535, 0.0.0.0/0)

Type: All TCP

Protocol: TCP

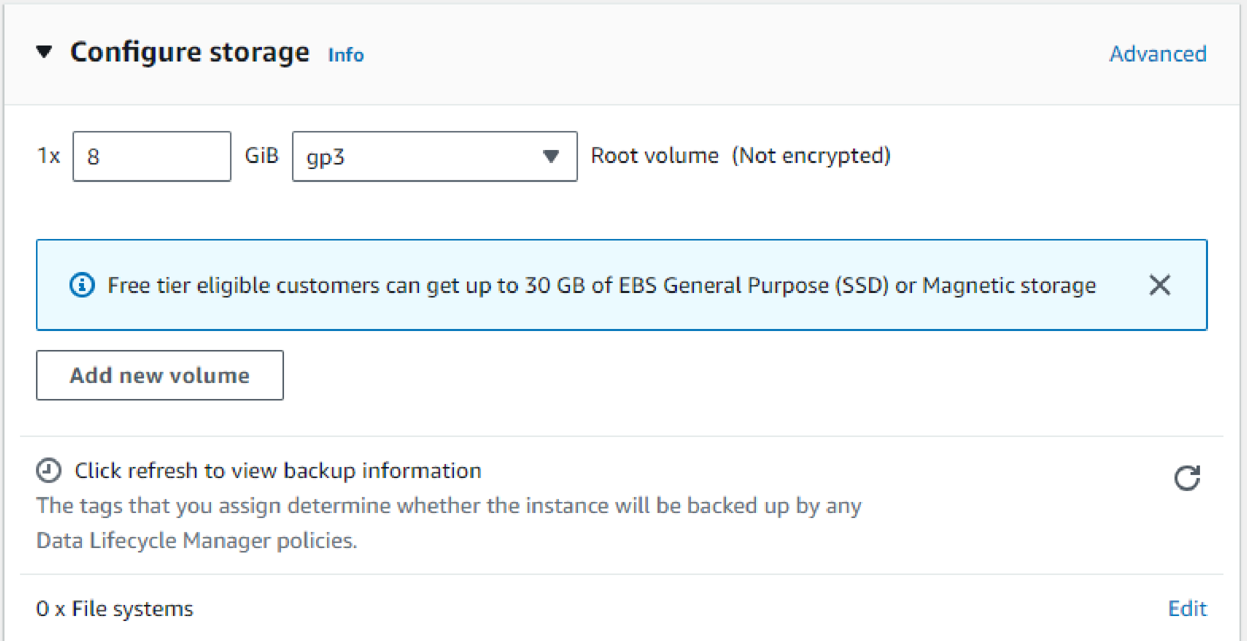
Port range: 0-65535

Source type: Custom

Source: 0.0.0.0/0

Description - *optional*: *e.g. SSH for admin desktop*

Storage Volume Keep 8 only Later on we will mount volume if needed.



▼ Configure storage Info Advanced

1x 8 GiB gp3 ▼ Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

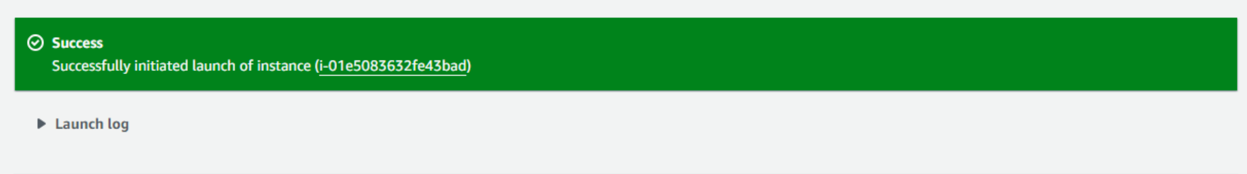
Add new volume

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

Check the Summary and then click on Launch Instance.

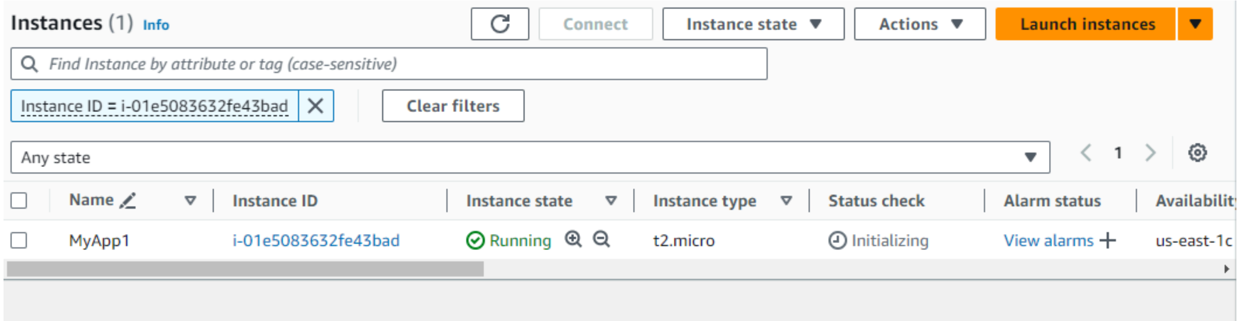


Success

Successfully initiated launch of instance (i-01e5083632fe43bad)

▶ Launch log

Click on instance and and you can see the instance details as below like its running or pending state.

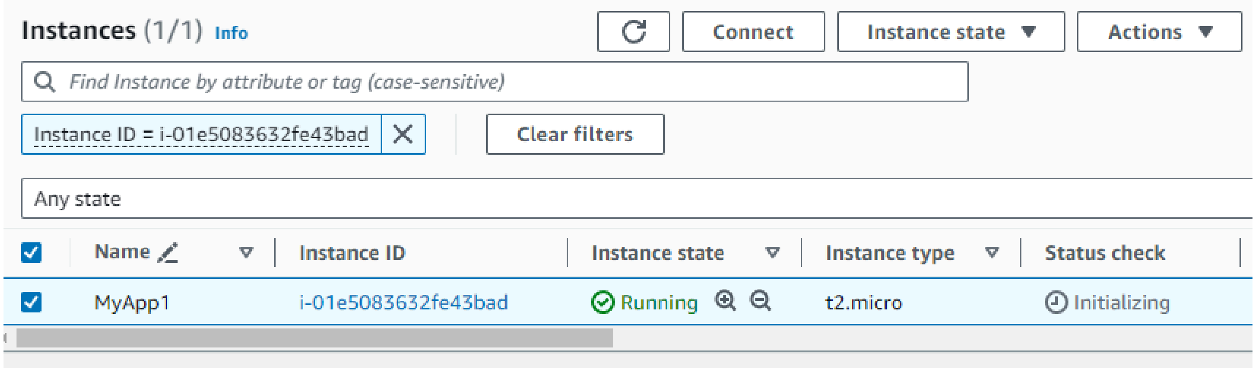


Instances (1) Info

Connect
Instance state ▼
Actions ▼
Launch instances ▼
Find Instance by attribute or tag (case-sensitive)
Instance ID = i-01e5083632fe43bad ✕
Clear filters
Any state ▼
< 1 >

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availabilit
□	MyApp1	i-01e5083632fe43bad	✓ Running	t2.micro	Initializing	View alarms +	us-east-1c

Now select you instance and click on Connect

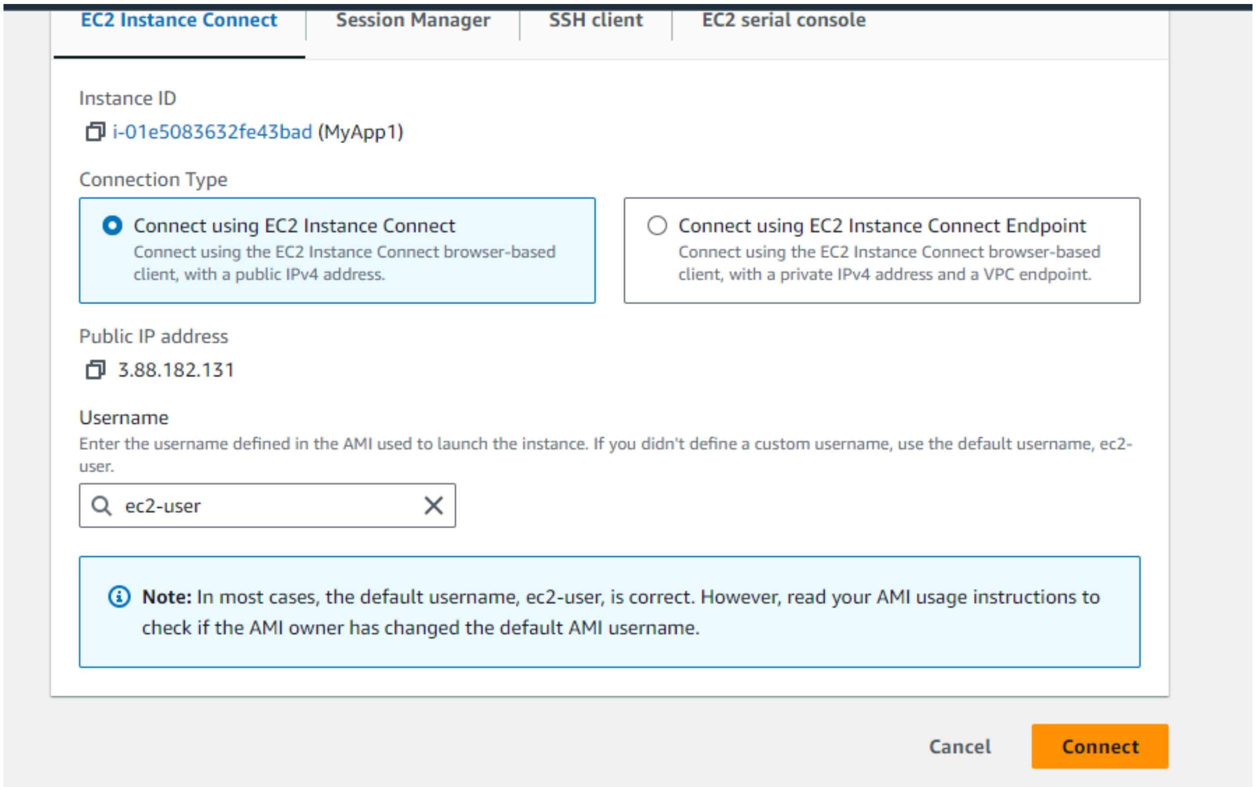


Instance ID = i-01e5083632fe43bad

Any state

☑	Name	Instance ID	Instance state	Instance type	Status check
☑	MyApp1	i-01e5083632fe43bad	Running	t2.micro	Initializing

Scroll down and click on Connect button which is available below.



Instance ID
i-01e5083632fe43bad (MyApp1)

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
3.88.182.131

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.

This is Direct connectivity to your instance, now let's connect from local system.

Create a folder named project and paste that .pem key pair file to that folder.

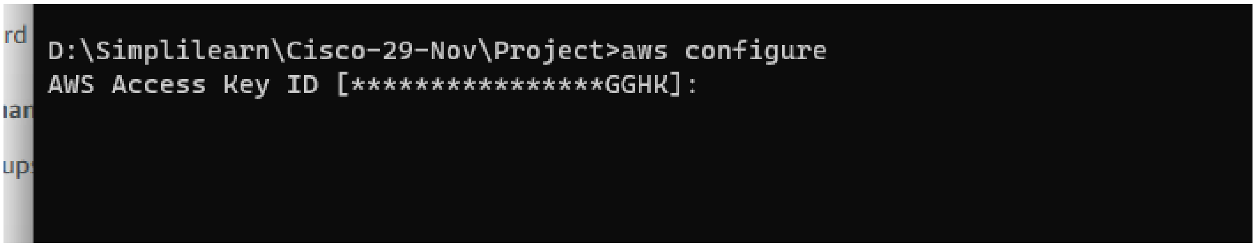
Go to the browser and search for amazon cli installation instructions.

https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

Or open this link, you can see the step of mac,windows and linux.

Once its installed check aws –version

If getting then let’s proceed with AWS configure.

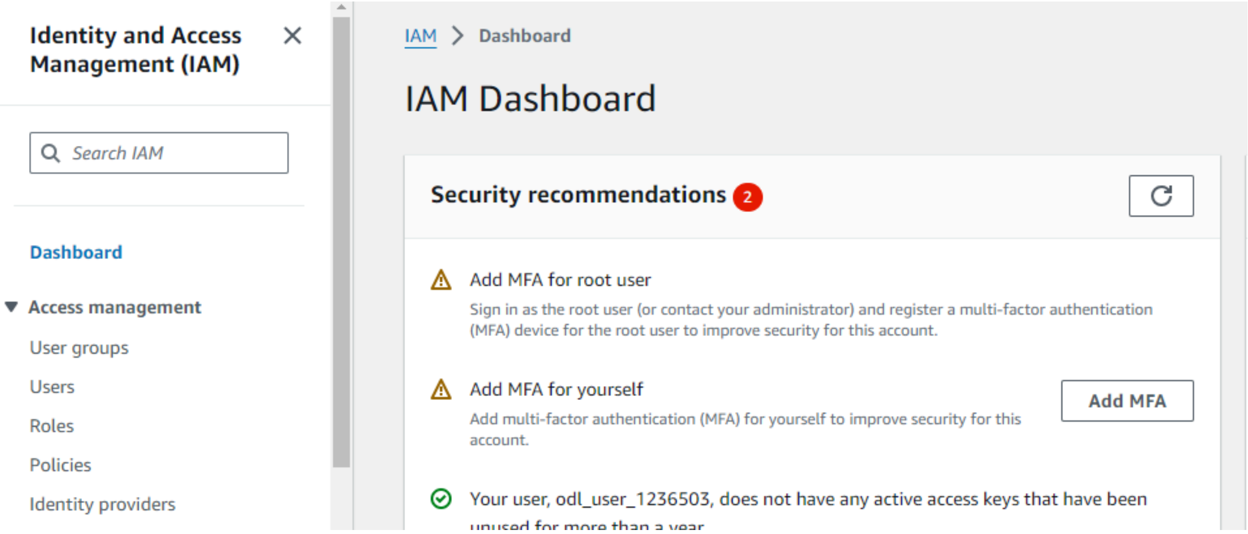


```
D:\Simplilearn\Cisco-29-Nov\Project>aws configure
AWS Access Key ID [****************GGHK]:
```

It will prompt you to enter Access Key

Let’s Generate Access Key

Search For IAM service and click on the same to open Dashboard



IAM Dashboard

Security recommendations 2

Add MFA for root user

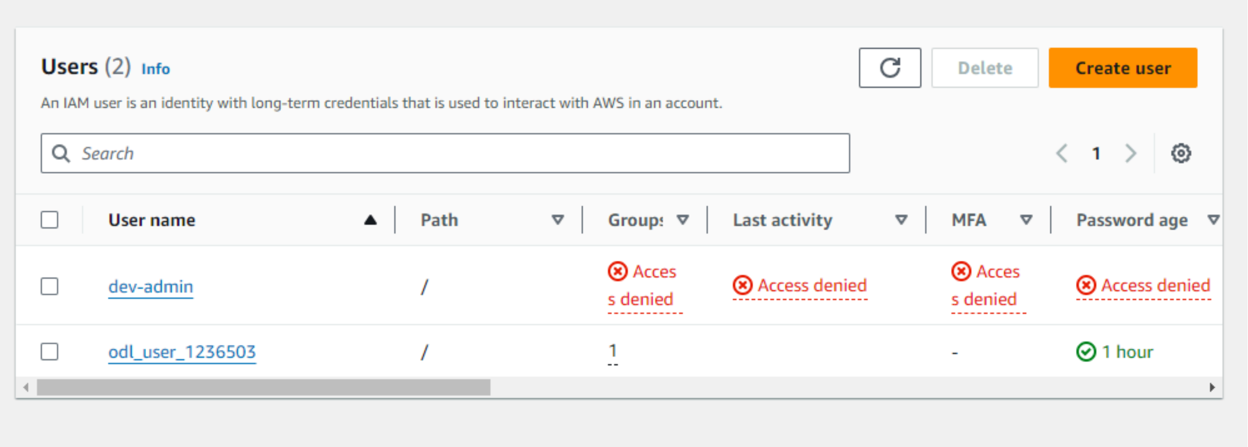
Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

Add MFA for yourself

Add multi-factor authentication (MFA) for yourself to improve security for this account.

Your user, odl_user_1236503, does not have any active access keys that have been unused for more than a year

Click on Users

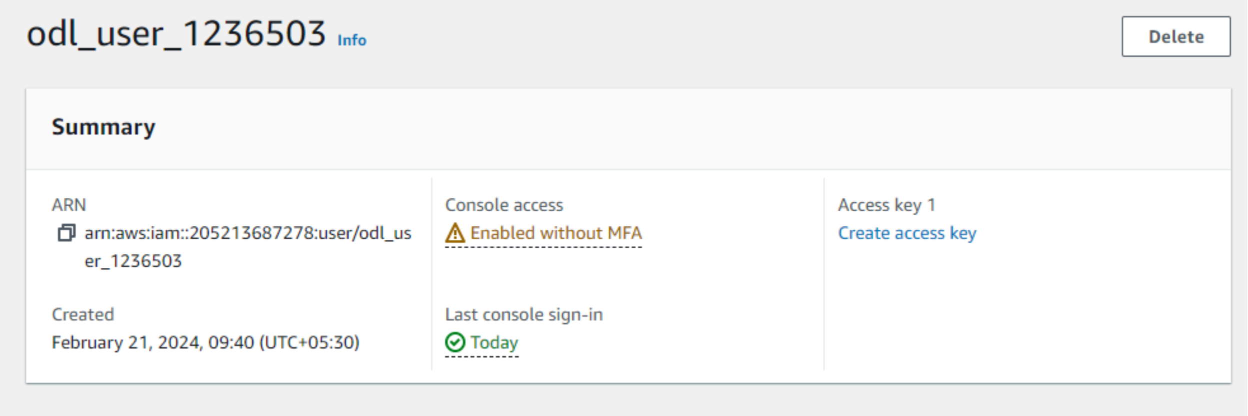


Users (2) Info

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

☐	User name ▲	Path	Groups	Last activity	MFA	Password age
☐	dev-admin	/	⊗ Access denied	⊗ Access denied	⊗ Access denied	⊗ Access denied
☐	odl_user_1236503	/	1		-	✓ 1 hour

Click on od_user



odl_user_1236503 Info

Summary

ARN
arn:aws:iam::205213687278:user/odl_user_1236503

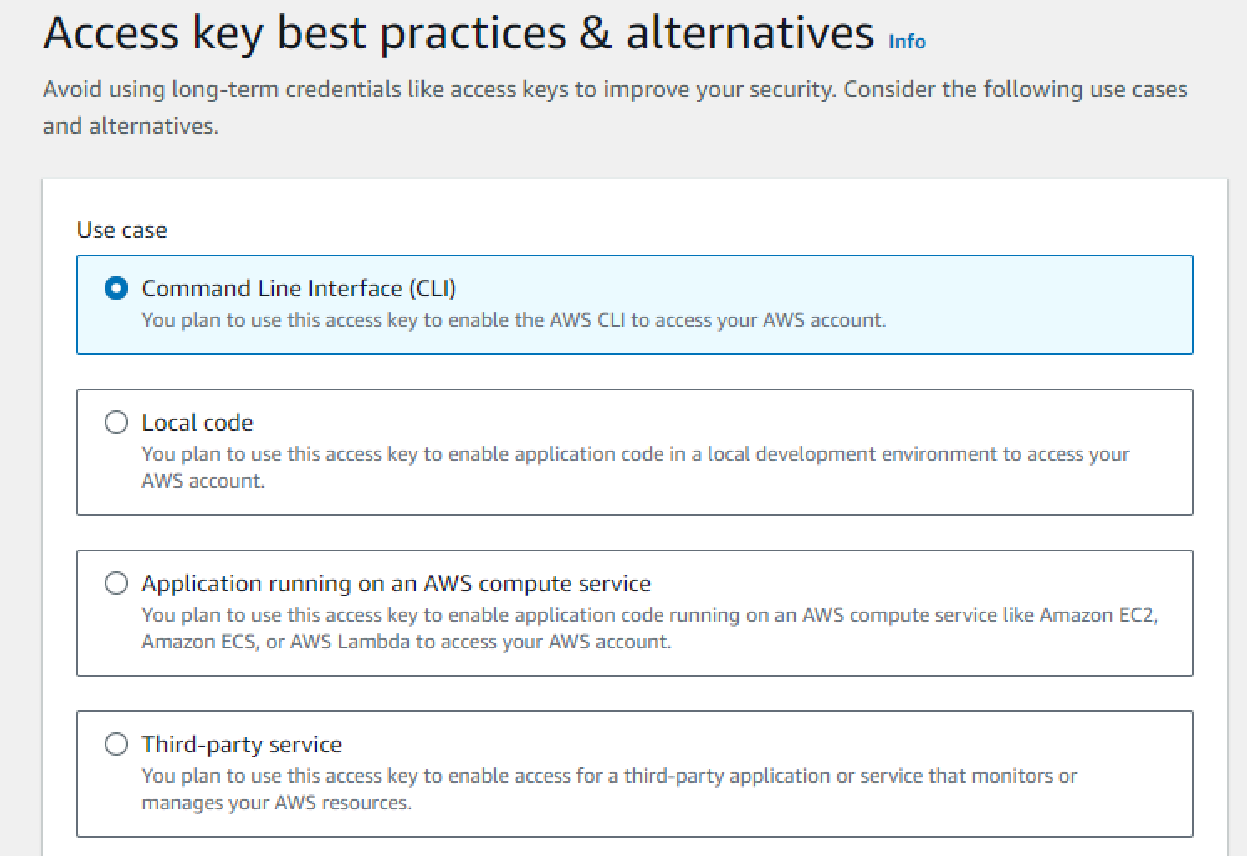
Console access
⚠ Enabled without MFA

Access key 1
Create access key

Created
February 21, 2024, 09:40 (UTC+05:30)

Last console sign-in
✓ Today

Click on Create Access Key



Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

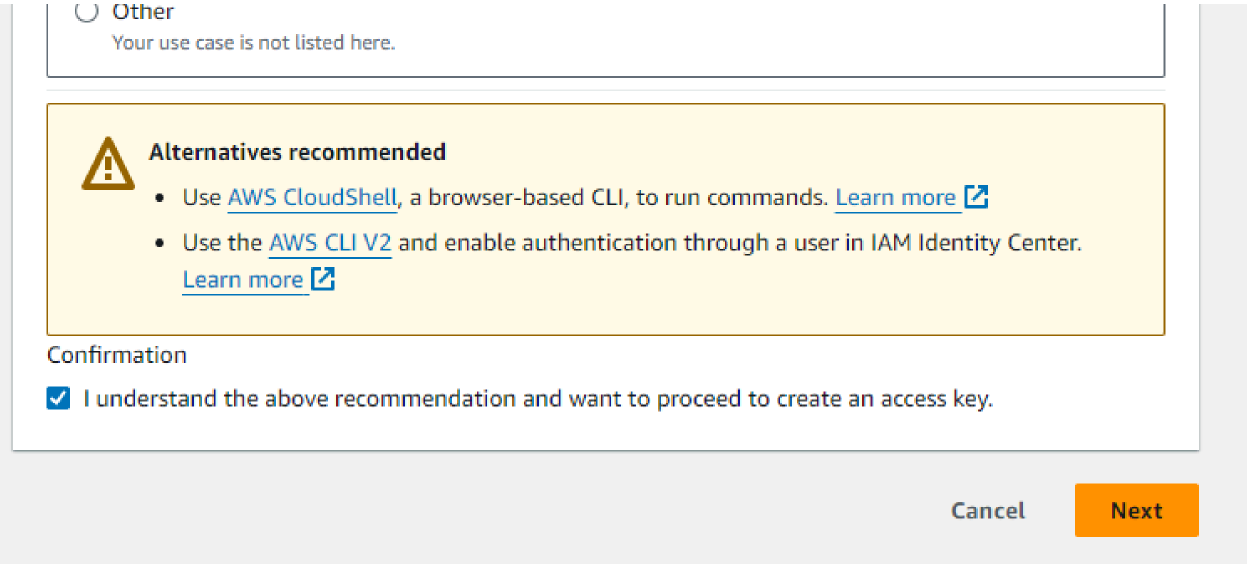
● Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

○ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Select CLI option



○ Other
Your use case is not listed here.

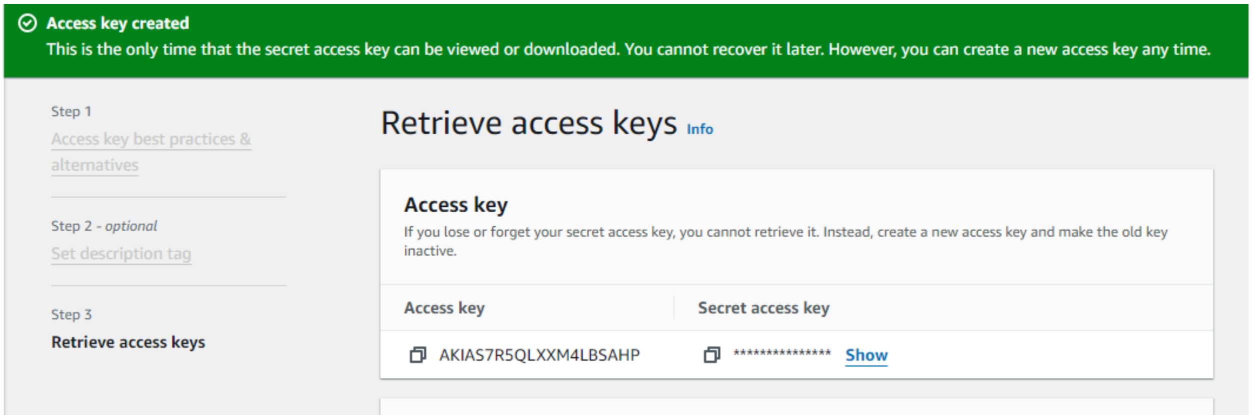
Alternatives recommended

- Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
- Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more

Confirmation

☑ I understand the above recommendation and want to proceed to create an access key.

Click on Next.
Click on create access key by giving any tag name.



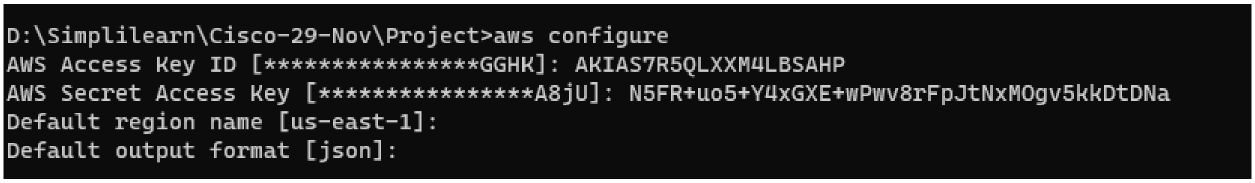
Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

Retrieve access keys Info

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAS7R5QLXXM4LBSAHP	*************** Show

Use this to configure in your system.



```
D:\Simplilearn\Cisco-29-Nov\Project>aws configure
AWS Access Key ID [****************GGHK]: AKIAS7R5QLXXM4LBSAHP
AWS Secret Access Key [****************A8jU]: N5FR+uo5+Y4xGXE+wPwv8rFpJtNxMOgv5kkDtDNa
Default region name [us-east-1]:
Default output format [json]:
```

AWS Configuration Done.