

# Assignment sheet for IAM

**Assignment 1 :-** Create an IAM user with username of your own wish and grant administrator policy.

The screenshot shows the AWS IAM 'Add user' console. The 'Set user details' step is active, indicated by a blue circle with the number 1. The 'User name' field is empty. Below it, there is a link to 'Add another user'. The 'Select AWS access type' section is visible, with two options: 'Access key - Programmatic access' and 'Password - AWS Management Console access'. The 'Access key' option is selected. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type\*

☐ Access key - Programmatic access  
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

☐ Password - AWS Management Console access  
Enables a password that allows users to sign-in to the AWS Management Console.

\* Required

Cancel Next: Permissions

The screenshot shows the AWS IAM 'Add user' console with the 'Set user details' step active. The 'User name' field is filled with 'Rockstar'. The 'Select AWS access type' section shows 'Password - AWS Management Console access' selected. The 'Console password' section shows 'Custom password' selected, with the password 'Rockstar1234' entered and the 'Show password' checkbox checked. The 'Require password reset' section shows 'User must create a new password at next sign-in' selected. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type\*

☐ Access key - Programmatic access  
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

☒ Password - AWS Management Console access  
Enables a password that allows users to sign-in to the AWS Management Console.

Console password\*

☐ Autogenerated password

☒ Custom password

Rockstar1234

☒ Show password

Require password reset

☒ User must create a new password at next sign-in  
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

\* Required

Cancel Next: Permissions

Services

Search

AWSServicesSearch[Alt+S]

GlobalSheet

Add user

12345

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group

Refresh

Search

Showing 1 result

| Group                                    | Attached policies   |
|--|---------------------|
| <input checked="" type="checkbox"/> NO 1 | AdministratorAccess |

Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

Create user without a permissions boundary

Use a permissions boundary to control the maximum user permissions

Select policy to set the permissions boundary

Create policy

Filter policies

Search

Showing 1021 results

| Policy name  | Type         | Used as |
|--|--------------|---------|
| <input type="radio"/> AccessAnalyzerServiceRolePolicy      | AWS managed  | None    |
| <input checked="" type="radio"/> AdministratorAccess       | Job function | None    |
| <input type="radio"/> AdministratorAccess-Ampify           | AWS managed  | None    |
| <input type="radio"/> AdministratorAccess-AmazonCloudWatch | AWS managed  | None    |
| <input type="radio"/> AdministratorAccess-AmazonEC2        | AWS managed  | None    |

Cancel

Previous

Next: Tags

Services

Search

AWSServicesSearch[Alt+S]

GlobalSheet

Add user

12345

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

| Key         | Value (optional) | Remove |
|-------------|------------------|--------|
| R1          | r134             | X      |
| Add new key |                  |        |

You can add 49 more tags.

Services

Search

AWSServicesSearch[Alt+S]

GlobalSheet

Add user

12345

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key

User details

|                        |   |
|------------------------|---|
| User name              | Rockstar  |
| AWS access type        | AWS Management Console access - with a password |
| Console password type  | Custom  |
| Require password reset | No  |
| Permissions boundary   | AdministratorAccess <a href="#">?</a>           |

Permissions summary

The user shown above will be added to the following groups.

| Type  | Name |
|-------|------|
| Group | NO 1 |

Tags

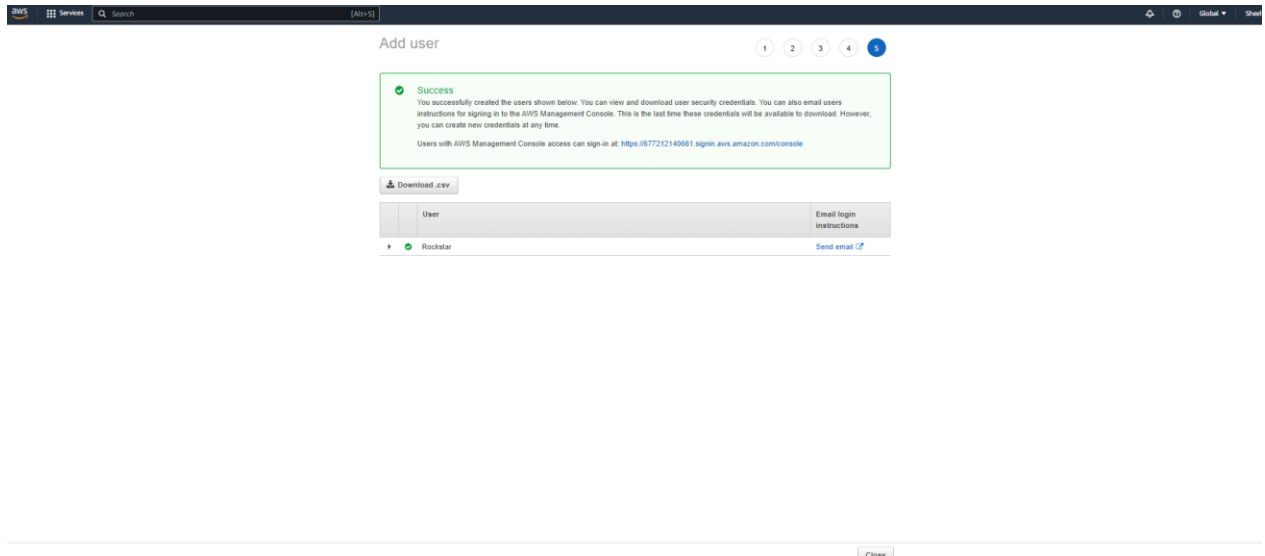
The new user will receive the following tag

| Key | Value |
|-----|-------|
| R1  | R134  |

Cancel

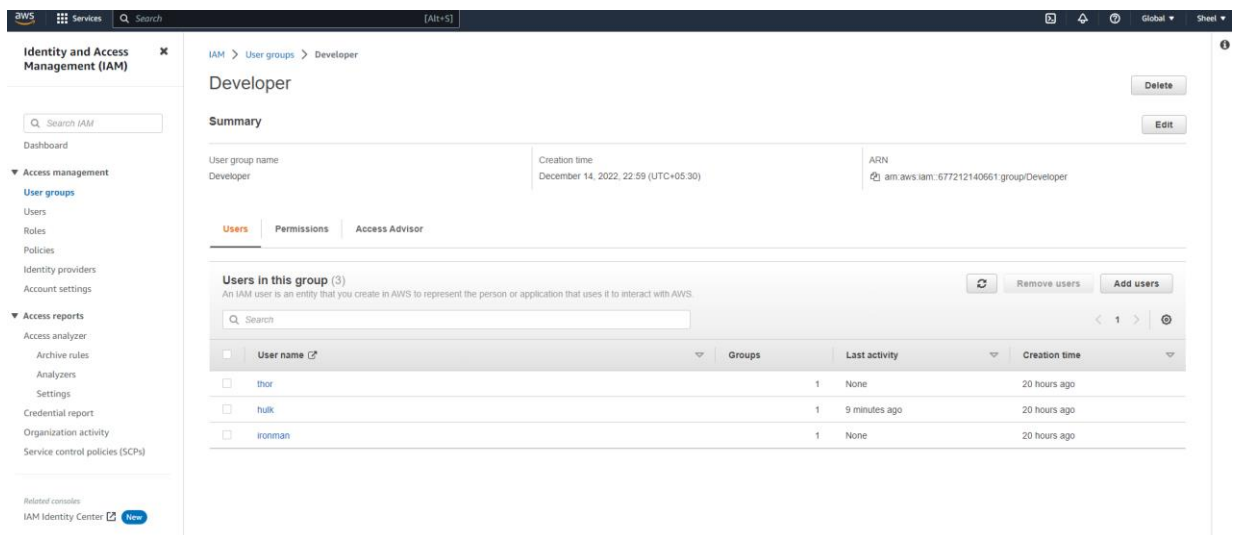
Previous

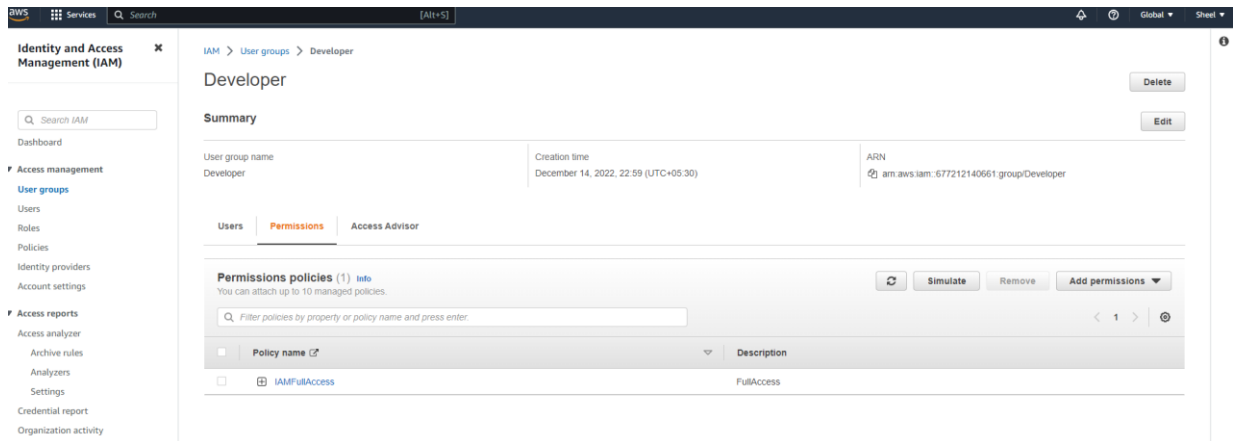
Create user



**Assignment 2 :-** Hello students, in this assignment you need to prepare a developers team of avengers.

- Create 3 IAM users of avengers and assign them in developer's groups with IAM policy.



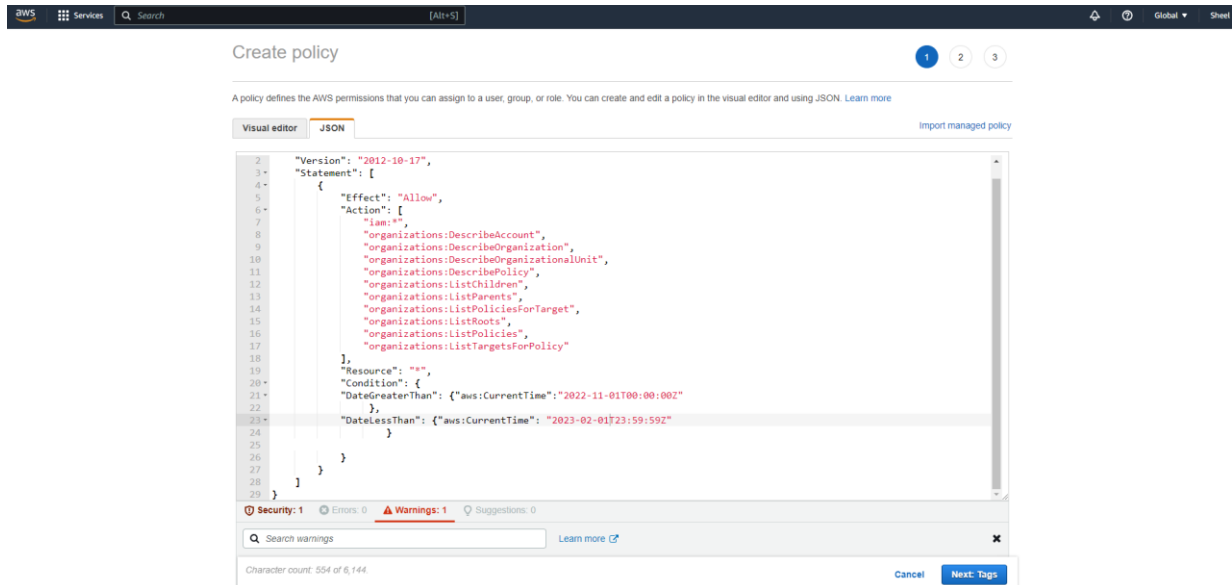


**Assignment 3 :-** Define a condition in policy for expiration like

```
"DateGreaterThan": { "aws:CurrentTime":  
"2020-04-01T00:00:00Z" },
```

```
    "DateLessThan": { "aws:CurrentTime":  
"2020-06-30T23:59:59Z" }
```

Define the span of 4 months as per your wish



## Create policy

### Review policy

Name\* Custom\_IAM

Use alphanumeric and '+=-\_@.~' characters. Maximum 128 characters.

Description Custom IAM with expiration policy of span of 4 months

Maximum 1000 characters. Use alphanumeric and '+=-\_@.~' characters.

#### Summary

Filter

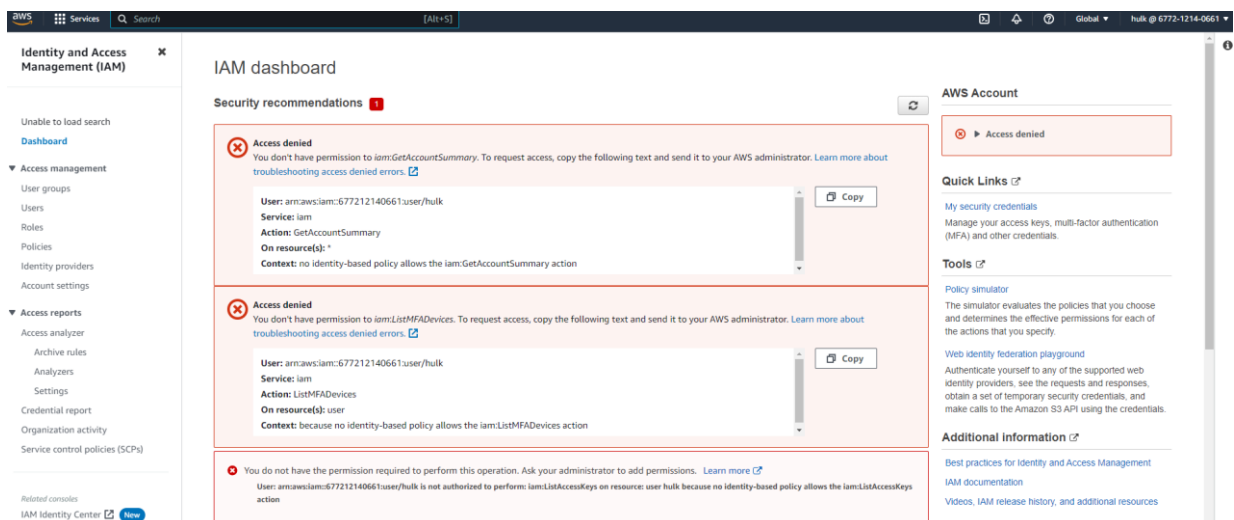
| Service                                      | Access level        | Resource      | Request condition |
|--|---------------------|---------------|-------------------|
| Allow (2 of 364 services) Show remaining 362 |                     |               |                   |
| IAM  | Full access         | All resources | Multiple          |
| Organizations                                | Limited: List, Read | All resources | Multiple          |

#### Tags

| Key | Value |
|-----|-------|
|-----|-------|

No tags associated with the resource.

As per the policy user can access IAM date starting from 01-11-2022 to 01-02-2023 but today is 02-02 so user can't access.




### Assignment 3 :- Prepare 15 authentic MCQ questions related to IAM.

- 1) Which statement best describes IAM?
  - a. IAM stands for Improvised Application Management, and it allows you to deploy and manage applications in the AWS Cloud.
  - b. IAM allows you to manage users, groups, roles, and their corresponding level of access to the AWS Platform.**
  - c. IAM allows you to manage users' passwords only. AWS staff must create new users for your organization. This is done by raising a ticket.
  - d. IAM allows you to manage permissions for AWS resources only
- 2) Which of the following is not a component of IAM?
  - a. Roles
  - b. Users
  - c. Organizational Units**
  - d. Groups
- 3) Which of the following is not a feature of IAM?
  - a. IAM allows you to setup biometric authentication, so that no passwords are required.**
  - b. IAM offers fine-grained access control to AWS resources.
  - c. IAM offers centralized control of your AWS account.
  - d. IAM integrates with existing active directory account allowing single sign-on.
- 4) By default a new user in IAM has permissions to log in to the AWS Console.
  - a. True
  - b. False**
- 5) Which of the following is not an IAM best practice?
  - a. Delete user accounts not in use
  - b. Attach policies to individual users.**
  - c. Manage permissions by adding users to groups.
  - d. Enable MFA on user accounts.
- 6) Name the service that is used to provide access control to aws?
  - a. EC2
  - b. IAM**
  - c. RDS
- 7) What will be the charges for using IAM?
  - a. IAM is offered at no additional charge.**
  - b. Its charged based on usage
  - c. It's charged based on the numbers of users created.

- 8) What is used to generate fine grained IAM policy based on User's use of Aws?
- a. **IAM access analyzer**
  - b. IAM access generator
  - c. AWS access analyzer
  - d. AWS access generator
- 9) What should you use if you want to grant access to your aws accounts by relying on short term credentials ?
- a. IAM policies
  - b. IAM users
  - c. Groups
  - d. **IAM roles**
- 10) Which policy is created and administrated by AWS and cover common use cases ?
- a. Customer managed policies
  - b. AWS created policies
  - c. **AWS managed policies**
- 11) If you create your own standalone policy in AWS, it is a type of
- a. AWS managed policies
  - b. **Customer managed policies**
  - c. AWS created policies
  - d. Customer created policy
- 12) Which policy is embedded in an IAM identity and inherent to the identity ?
- a. **Inline policy**
  - b. Inherent policy
  - c. Resource based policy
- 13) If you can define permission based on tags , what is the type of access control ?
- a. **Attribute-based access control(ABAC)**
  - b. Tag-based access control
  - c. Role-based access control
- 14) Which tool is used to test and troubleshoot identity-based and resource-based policies, IAM permissions boundaries ?
- a. **IAM policy simulator**
  - b. IAM policy troubleshooter
  - c. IAM policy tester
- 15) What are IAM policies?
- a. AWS service performable action
  - b. **JSON document to define user, resource or roles permission**
  - c. Rules to set up password for IAM users

## Assignment 4 :- Launch your linux instance in IAM and update your machine.



Sign in

☐ Root user  
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☒ IAM user  
User within an account that performs daily tasks. [Learn more](#)


Account ID (12 digits) or account alias

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.


☐ New to AWS?

Create a new AWS account



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English



Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

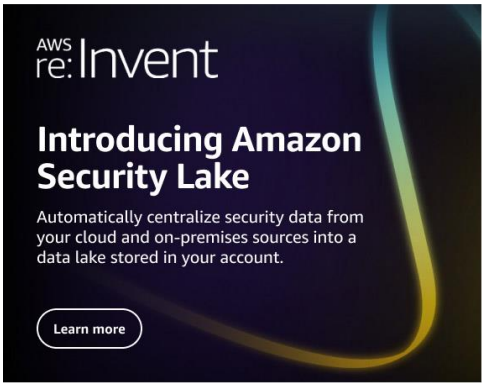
Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)



English

[Terms of Use](#) [Privacy Policy](#) © 1995-2022, Amazon Web Services, Inc. or its affiliates.

EC2 > Instances > Launch an instance

Launch an instance [Info](#)

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 [Info](#)


Name

Add additional tags


▼ 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


Quick Start




Amazon Linux




macOS




Ubuntu




Windows



Red Hat



S



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Linux 2 AMI (HVM) - Kernel 5.10. SSD Volume Type

Free tier eligible

▼ Summary

Number of instances [Info](#)

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...[read more](#)  
ami-074dc0a6f6c764218

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

③ Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

×


Cancel

Launch instance



## ▼ 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

AMI from catalog

Quick Start

Amazon Machine Image (AMI)

amzn2-ami-kernel-5.10-hvm-  
2.0.20221103.3-x86\_64-gp2  
ami-074dc0a6f6c764218

Free tier eligible

Verified provider



Browse more AMIs

Including AMIs from  
AWS, Marketplace and  
the Community

| Catalog            | Published                        | Architecture | Virtualization | Root device<br>type | ENA Enabled |
|--------------------|----------------------------------|--------------|----------------|---------------------|-------------|
| Quickstart<br>AMIs | 2022-11-<br>14T23:11:50.0<br>00Z | x86_64       | hvm            | ebs                 | Yes         |

### Create key pair



Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

Enter key pair name

The name can include upto 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 (Not supported for Windows instances)

Private key file format

- ☒ .pem  
For use with OpenSSH
- ☐ .ppk  
For use with PuTTY

Cancel

Create key pair

## ▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0124 USD per Hour

On-Demand Windows pricing: 0.017 USD per Hour

Free tier eligible

[Compare instance types](#)

## ▼ 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*

linux

[Create new key pair](#)

## ▼ Network settings [Info](#)

[Edit](#)

Network [Info](#)

vpc-0d3ab5a20c883ebf5

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-3' 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

☒ Allow HTTP traffic from the internet

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

## ▼ Configure storage [Info](#)

[Advanced](#)

1x

8

GiB

gp2

Root volume (Not encrypted)

[Add new volume](#)

0 x File systems

[Edit](#)

[illegible]

```
[root@ip-172-31-7-171 ec2-user]# systemctl start httpd
[root@ip-172-31-7-171 ~]# cd /var/www/html/
[root@ip-172-31-7-171 html]# touch index.html
[root@ip-172-31-7-171 html]# ls
index.html
[root@ip-172-31-7-171 html]# vi index.html
```