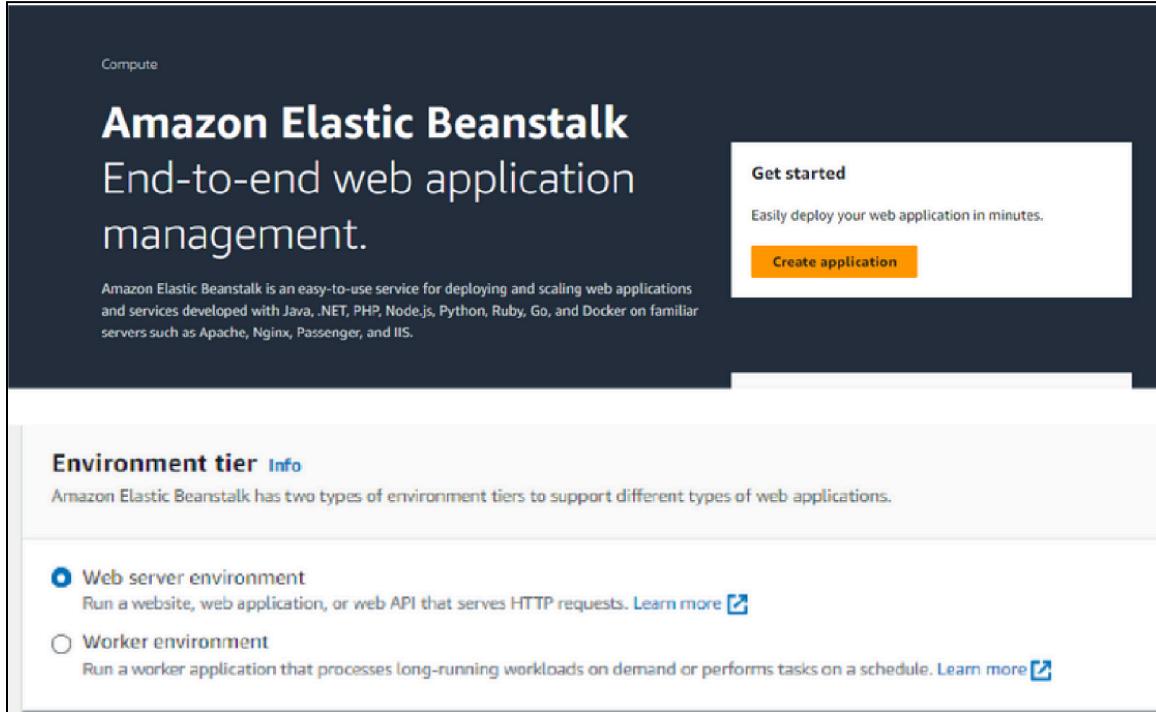


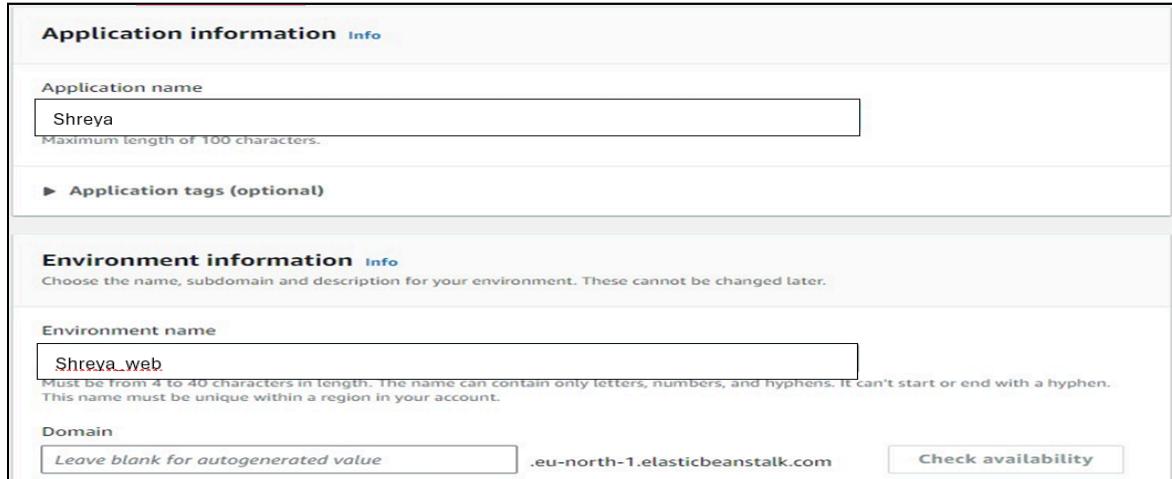
Experiment.2

Aim: To Build Your Application using AWS CodeBuild and Deploy on S3 / SEBS using AWS CodePipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy.

Using elastic Beanstalk-



The screenshot shows the Amazon Elastic Beanstalk landing page. At the top, it says "Compute" and "Amazon Elastic Beanstalk End-to-end web application management." Below this, a description states: "Amazon Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS." To the right, there is a "Get started" section with a "Create application" button. The main content area is titled "Environment tier" with a "Info" link. It says: "Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications." There are two options: "Web server environment" (selected) and "Worker environment". Both options have a "Learn more" link.



The screenshot shows the "Create New Application" form in the Amazon Elastic Beanstalk console. The first section is "Application information" with an "Info" link. It has a field for "Application name" containing "Shreya", with a note: "Maximum length of 100 characters." The next section is "Environment information" with an "Info" link. It has a field for "Environment name" containing "Shreya_web", with notes: "Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account." Below this is a "Domain" field with "Leave blank for autogenerated value" and ".eu-north-1.elasticbeanstalk.com", and a "Check availability" button.

Choose pipeline settings Info

Step 1 of 5

Pipeline settings

Pipeline name
Enter the pipeline name. You cannot edit the pipeline name after it is created.

No more than 100 characters

Pipeline type

ⓘ You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.

Execution mode
Choose the execution mode for your pipeline. This determines how the pipeline is run.

Superseded
A more recent execution can overtake an older one. This is the default.

Queued (Pipeline type V2 required)
Executions are processed one by one in the order that they are queued.

Parallel (Pipeline type V2 required)
Executions don't wait for other runs to complete before starting or finishing.

Service role

New service role
Create a service role in your account

Existing service role
Choose an existing service role from your account

Role name

Type your service role name

Allow AWS CodePipeline to create a service role so it can be used with this new pipeline

Platform Info

Platform type

Managed platform
Platforms published and maintained by Amazon Elastic Beanstalk. [Learn more](#) 

Custom platform
Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

PHP 

Platform branch

PHP 8.3 running on 64bit Amazon Linux 2023 

Platform version

4.3.2 (Recommended) 

Application code Info

Sample application

Existing version
Application versions that you have uploaded.

Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.

Presets Info

Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default values.

Configuration presets

Single instance (free tier eligible)

Single instance (using spot instance)

High availability

High availability (using spot and on-demand instances)

Custom configuration

Developer Tools > Connections > Create connection

Create a connection Info

Create GitHub App connection Info

Connection name

Tags - optional

Connect to GitHub

CloudShell Feedback Privacy Terms Cookie preferences

Configure service access Info

Service access

IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. [Learn more](#)

Service role Create and use new service role Use an existing service role

Service role name
Enter the name for an IAM role that Elastic Beanstalk will create to assume as a service role. Beanstalk will attach the required managed policies to it.

[View permission details](#)

EC2 key pair
Select an EC2 key pair to securely log in to your EC2 instances. [Learn more](#)

EC2 instance profile
Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

[View permission details](#)

[Cancel](#) [Skip to review](#) [Previous](#) **Next**

Developer Tools > Connections > Create connection

Create a connection Info

Create GitHub App connection Info

Connection name
githubwebapp1

▶ Tags - optional

Connect to GitHub

CloudShell Feedback Privacy Terms Cookie preferences

This screenshot shows the 'Create a connection' page for a GitHub App in the AWS Lambda console. The top navigation bar includes 'Developer Tools', 'Connections', and 'Create connection'. The main section is titled 'Create GitHub App connection' with an 'Info' link. It has a 'Connection name' field containing 'githubwebapp1'. Below it is a 'Tags - optional' section. At the bottom right is a large orange 'Connect to GitHub' button.

Developer Tools > Connections > Create connection

Beginning July 1, 2024, the console will create connections with codeconnections in the resource ARN. Resources with both service prefixes will continue to display in the console. [Learn more](#) X

Connect to GitHub

GitHub connection settings Info

Connection name
githubwebapp1

App installation - optional
Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.
Q 53746790 X or Install a new app

▶ Tags - optional

Connect

This screenshot shows the 'Connect to GitHub' page in the AWS Lambda console. A blue banner at the top informs users that starting July 1, 2024, connections will be created with 'codeconnections' in the resource ARN. It includes a 'Learn more' link and a close 'X' button. The main form is titled 'GitHub connection settings' with an 'Info' link. It has a 'Connection name' field with 'githubwebapp1'. Below it is an 'App installation - optional' section with a search input 'Q 53746790', a delete 'X' button, and an 'Install a new app' button. There is also a 'Tags - optional' section and a 'Connect' button at the bottom right.

Source

Source provider

This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.

GitHub (Version 2) ▾



New GitHub version 2 (app-based) action

To add a GitHub version 2 action in CodePipeline, you create a connection, which uses GitHub Apps to access your repository. Use the options below to choose an existing connection or create a new one. [Learn more](#)

Connection

Choose an existing connection that you have already configured, or create a new one and then return to this task.

arn:aws:codeconnections:eu-north-1:011528263675:connection/3ff01730-e1... X or [Connect to GitHub](#)



Ready to connect

Your GitHub connection is ready for use.

Default branch

Default branch will be used only when pipeline execution starts from a different source or manually started.

master X

Output artifact format

Choose the output artifact format.

CodePipeline default

AWS CodePipeline uses the default zip format for artifacts in the pipeline. Does not include Git metadata about the repository.

Full clone

AWS CodePipeline passes metadata about the repository that allows subsequent actions to do a full Git clone. Only supported for AWS CodeBuild actions.

Trigger

Trigger type

Choose the trigger type that starts your pipeline.

No filter

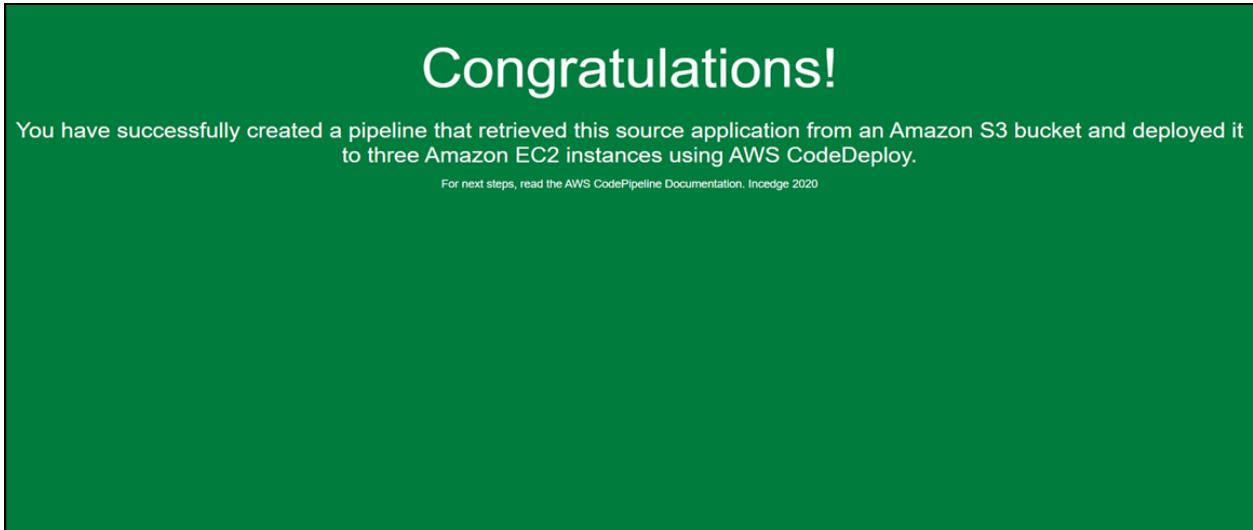
Starts your pipeline on any push and clones the HEAD.

Specify filter

Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.

Do not detect changes

Don't automatically trigger the pipeline.



Pipeline type: V2 Execution mode: QUEUED

Source Succeeded
Pipeline execution ID: [9752de3e-526c-4b2b-b19a-41aa6526a5d8](#)

Source
[GitHub \(Version 2\)](#)

Succeeded - 5 days ago
[8fd5da54](#)

[View details](#)

[8fd5da54](#) Source: Update README.md

[Disable transition](#)

Deploy Succeeded
Pipeline execution ID: [9752de3e-526c-4b2b-b19a-41aa6526a5d8](#)

Deploy
[AWS Elastic Beanstalk](#)

Succeeded - 5 days ago
[View details](#)

[Start rollback](#)

Using S3 bucket-

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type Info

General purpose
Recommended for most use cases and access patterns.
General purpose buckets are the original S3 bucket type.
They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory - New
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info
Shreya_bean

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming Info

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

```
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-31-41-61:/home/ubuntu# systemctl status apache2
● apache2.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
    Active: active (running) since Sun 2024-08-18 12:30:09 UTC; 30s ago
      Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2442 (apache2)
     Tasks: 55 (limit: 1130)
    Memory: 5.4M (peak: 5.7M)
       CPU: 40ms
      CGroup: /system.slice/apache2.service
              └─2442 /usr/sbin/apache2 -k start
                  ├─2445 /usr/sbin/apache2 -k start
                  ├─2446 /usr/sbin/apache2 -k start

Aug 18 12:30:09 ip-172-31-41-61 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 18 12:30:09 ip-172-31-41-61 systemd[1]: Started apache2.service - The Apache HTTP Server.
root@ip-172-31-41-61:/home/ubuntu# cd /var/www/html
root@ip-172-31-41-61:/var/www/html#
```

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose Add files or Add folder.

Files and folders (1 Total, 315.0 B)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	index.html	-	text/html

Application code Info

Sample application

Existing version
Application versions that you have uploaded.

Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.

Presets Info

Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default values.

Configuration presets

Single instance (free tier eligible)

Single instance (using spot instance)

High availability

High availability (using spot and on-demand instances)

Custom configuration

Cancel **Next**

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through any public bucket or access point policies

This setting prevents public and cross-account access to buckets and objects through any public bucket or access point policies.

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.



Enabling ACLs turns off the bucket owner enforced setting for Object Ownership

Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

I acknowledge that ACLs will be restored.

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

Disable

Enable

Hosting type

Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

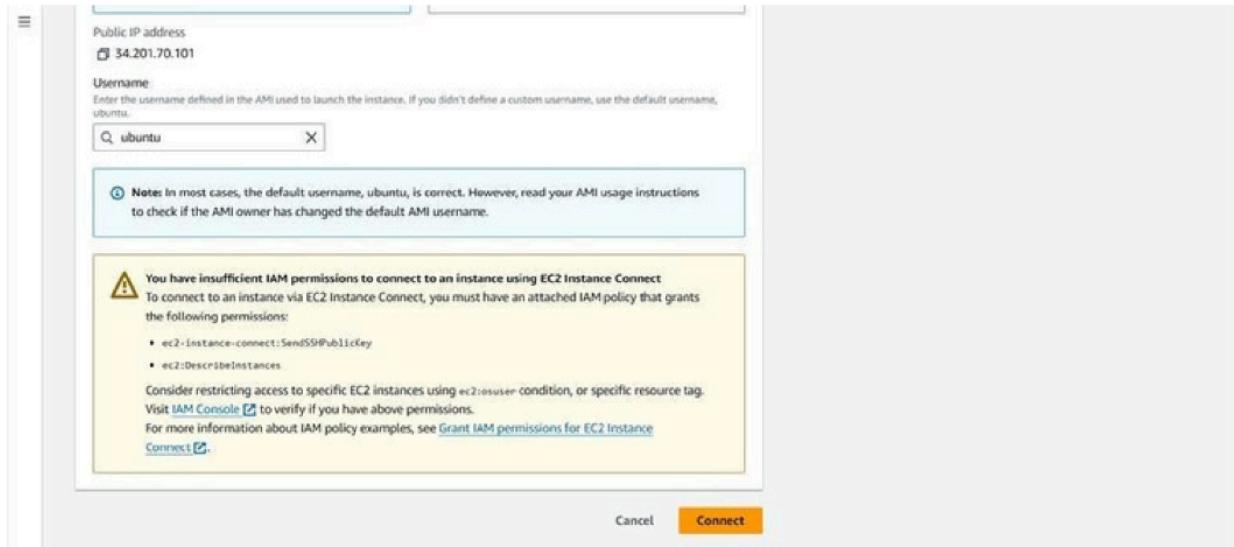
Index document
Specify the home or default page of the website.

index.html

Using EC2

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with links like AWS Console Home, EC2 Global View, Events, Console-to-Code, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The Instances link is currently selected. The main content area has a header 'Instances (1/1) info'. Below it is a table with one row, showing details for an instance named 'dynamic-server'. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Put. The instance is listed as 'Running' (t2.micro, 2/2 checks passed, us-east-1). Below the table, there's a detailed view for the 'dynamic-server' instance, showing its instance ID (i-0ecbd8d07a55bd2e3), public IPv4 address (34.201.70.101), private IP4 address (172.31.85.104), public IPv4 DNS (ec2-54-201-70-101.compute-1.amazonaws.com), and private IP4 DNS (ip-172-31-85-104.ec2.internal). It also shows its hostname type (IP name: ip-172-31-85-104.ec2.internal), answer private resource DNS name (IPv4 [A]), instance type (t2.micro), and elastic IP addresses (none).

Shreya Sawant D15A 54



See "man sudo_root" for details.

```
ubuntu@ip-172-31-41-61:~$ sudo su
root@ip-172-31-41-61:/home/ubuntu# sudo apt install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ip-172-31-41-61:/home/ubuntu# sudo apt-get update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [294 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [68.1 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [3768 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [250 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [108 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [9412 B]
```

EC2 > Security Groups > sg-0e7811c687e701e30 - launch-wizard-7

sg-0e7811c687e701e30 - launch-wizard-7

Actions ▾

Details			
Security group name <input type="checkbox"/> launch-wizard-7	Security group ID <input type="checkbox"/> sg-0e7811c687e701e30	Description <input type="checkbox"/> launch-wizard-7 created 2024-08-18T11:25:33.225Z	VPC ID <input type="checkbox"/> vpc-08963bc0f8afcd789 <input checked="" type="checkbox"/>
Owner <input type="checkbox"/> 608111999703	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (1)

< 1 >

Details			
Security group name <input type="checkbox"/> launch-wizard-9	Security group ID <input type="checkbox"/> sg-0896d82a58154b33d	Description <input type="checkbox"/> launch-wizard-9 created 2024-08-18T12:21:13.480Z	VPC ID <input type="checkbox"/> vpc-08963bc0f8afcd789 <input checked="" type="checkbox"/>
Owner <input type="checkbox"/> 608111999703	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules **Outbound rules** Tags

Outbound rules (1)

< 1 >

Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/> -	sgr-06dd7ee61f83e4e88	IPv4	All traffic	All

Details			
Security group name <input type="checkbox"/> launch-wizard-9	Security group ID <input type="checkbox"/> sg-0896d82a58154b33d	Description <input type="checkbox"/> launch-wizard-9 created 2024-08-18T12:21:13.480Z	VPC ID <input type="checkbox"/> vpc-08963bc0f8afcd789 <input checked="" type="checkbox"/>
Owner <input type="checkbox"/> 608111999703	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules **Outbound rules** Tags

Outbound rules (1)

< 1 >

Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/> -	sgr-06dd7ee61f83e4e88	IPv4	All traffic	All



👕 Order Your Customized T-Shirt 🤪

T-Shirt Details

Tagline on the Shirt:

Color:

Size:

Quantity:

Delivery Date:

Delivery Details 🎁

Recipient's name:

Address: