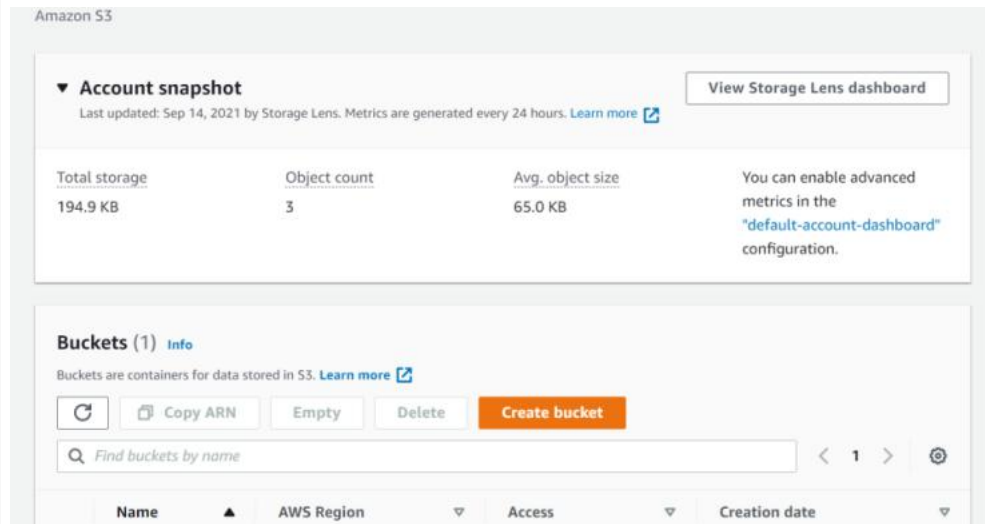


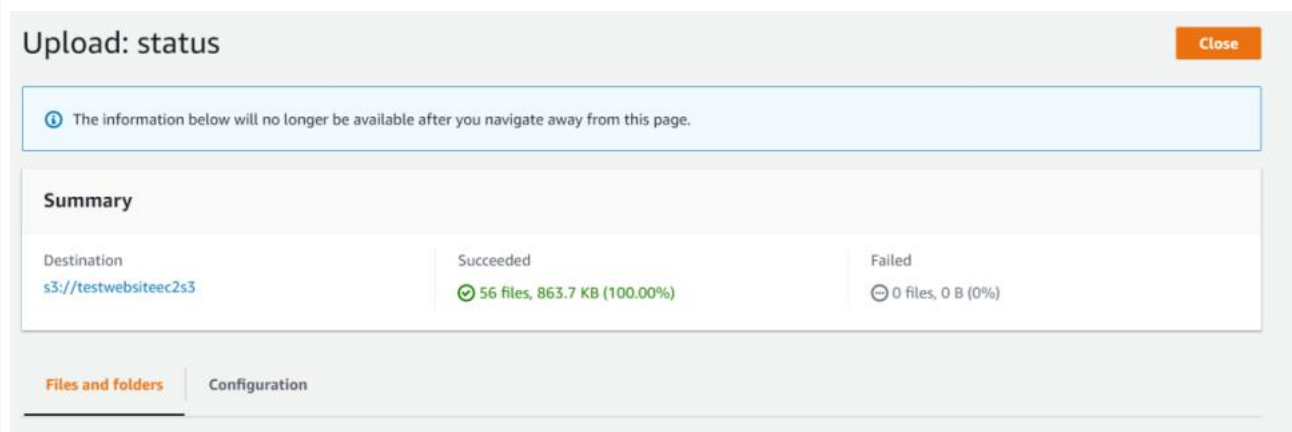
Launching a website on EC2 instance with S3 for static content and ALB and ASG for load balancing and auto-scaling respectively

By: Rohit Sah

Create an S3 bucket first



Upload the files in the s3 bucket





Now create an EC2 role for the instances


Create role


1234

Select type of trusted entity

 **AWS service**
EC2, Lambda and others

 **Another AWS account**
Belonging to you or 3rd party

 **Web identity**
Cognito or any OpenID provider

 **SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

* Required

Cancel

Next: Permissions

Select the policy for the role

Create role

1234

▼ Attach permissions policies

Choose one or more policies to attach to your new role.







Create policy

↺

Filter policies ▼

Q s3

Showing 9 results

	Policy name ▼	Used as
<input type="checkbox"/>	▶  AmazonDMSRedshiftS3Role	None
<input checked="" type="checkbox"/>	▶  AmazonS3FullAccess	None
<input type="checkbox"/>	▶  AmazonS3ObjectLambdaExecutionRolePolicy	None
<input type="checkbox"/>	▶  AmazonS3OutpostsFullAccess	None
<input type="checkbox"/>	▶  AmazonS3OutpostsReadOnlyAccess	None
<input type="checkbox"/>	▶  AmazonS3ReadOnlyAccess	None

* Required

Cancel

Previous

Next: Tags

Give a name to the role

Create role

1

2

3

4

Review

Provide the required information below and review this role before you create it.

Role name*

S3FullAccess

Use alphanumeric and '+,=, @, -, _' characters. Maximum 64 characters.

Role description


Allows EC2 instances to call AWS services on your behalf.

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

Trusted entities

AWS service: ec2.amazonaws.com

Policies



 AmazonS3FullAccess [↗](#)

* Required

Cancel

Previous

Create role

We can see that the role has been created

IAM > Roles

Roles (Selected 1/6) Info

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.


↺

Delete

Create role

Q Search

< 1 > ⚙

	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	25 days ago
<input type="checkbox"/>	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	25 days ago
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/>	DemoRoleForEC2	AWS Service: ec2	31 days ago
<input checked="" type="checkbox"/>	S3FullAccess	AWS Service: ec2	-

Now we create a security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name

ec2sg

Name cannot be edited after creation.

Description

ec2 security group

VPC

vpc-fd905f96

Inbound rules

Type	Protocol	Port range	Source	Description - optional	
SSH	TCP	22	Anywhere...		Delete
				0.0.0.0/0	
HTTP	TCP	80	Anywhere...		Delete
				0.0.0.0/0	
HTTPS	TCP	443	Anywhere...		Delete
				0.0.0.0/0	

We can see that the security group has been created

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Security group (sg-046e1598b1b6e9f54 | ec2sg) was created successfully

Details

EC2 > Security Groups > sg-046e1598b1b6e9f54 - ec2sg

sg-046e1598b1b6e9f54 - ec2sg

Details

Security group name	Security group ID	Description	VPC ID
ec2sg	sg-046e1598b1b6e9f54	ec2 security group	vpc-fd905f96
Owner	Inbound rules count	Outbound rules count	
809386103928	3 Permission entries	1 Permission entry	

Inbound rules

Outbound rules

Tags

Now we create a key pair

Create key pair

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

ec2s3keypair

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

Key pair type

☒ RSA

☐ ED25519

Private key file format

☐ .pem

For use with OpenSSH

☒ .ppk

For use with PuTTY

Tags (Optional)

No tags associated with the resource.

Add tag

You can add 50 more tags.

Now we create a ALB

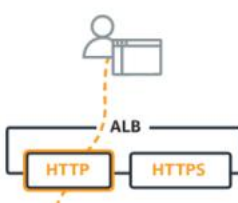
EC2 > Load balancers > Select load balancer type

Select load balancer type

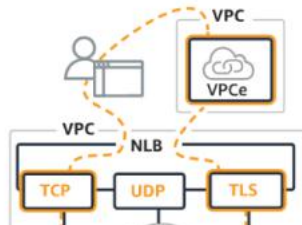
A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types


Application Load Balancer



Network Load Balancer



Gateway Load Balancer



Create Application Load Balancer [Info](#)

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

► How Application Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and cannot be changed after the load balancer is created.

DemoALB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme [Info](#)

Scheme cannot be changed after the load balancer is created.

☒ Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ Internal

An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type [Info](#)

Select the type of IP addresses that your subnets use.

☒ IPv4

Recommended for internal load balancers.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

vpc-fd905f96
IPv4: 172.31.0.0/16

Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection. Subnets cannot be removed after the load balancer is created, but additional subnets can be added. Availability Zones that are not supported by the load balancer or the VPC are disabled. At least two subnets must be specified.

☒ ap-south-1a

Subnet

subnet-6574810e

IPv4 settings

Assigned by AWS

☒ ap-south-1b

Subnet

subnet-0296cc4e

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

Select security groups

[Create new security group](#)

default sg-3342b44f
VPC: vpc-fd905f96

Listeners and routing [Info](#)

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

▼ Listener HTTP:80

Remove

Protocol

HTTP

Port

80

1-65535

Default action [Info](#)

Forward to

Select a target group

[Create target group](#)

Add listener

Create a target group for the ALB

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

☒ Instances

- Supports load balancing to instances within a specific VPC.

☐ IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.

☐ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

☐ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

PlumTargetGroup

Configure the ALB

Security groups

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

Select security groups

Create new security group

ec2sg sg-046e1598b1b6e9f54 VPC: vpc-fd905f96

Listeners and routing

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

▼ Listener HTTP:80

Remove

Protocol HTTP Port 80

Default action

Forward to DemoTargetGroup

Target type: Instance, IPv4

HTTP

Create target group

Add listener

Create an ASG for the application

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - required

DemoTemplate

Must be unique to this account. Max 128 chars. No spaces or special characters like %, ", '.

Template version description

templatedemo

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

☒ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ Template tags

▶ Source template

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ Amazon machine image (AMI) - required [Info](#)

AMI - required

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ Amazon machine image (AMI) - required [Info](#)

AMI - required

Amazon Linux 2 AMI (HVM), SSD Volume Type

ami-041b8256ad0f2081c

Catalog: Quick Start virtualization: hvm architecture: 64-bit (x86)

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

Free tier eligible

On-Demand Linux pricing: 0.0124 USD per Hour

On-Demand Windows pricing: 0.017 USD per Hour

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

ec2s3keypair

Create new key pair

▼ Network settings

▼ Network settings

Networking platform [Info](#)

☒ Virtual Private Cloud (VPC)
Launch into a virtual network in your own logically isolated area within the AWS Cloud

☐ EC2-Classic
Launch into a single flat network that you share with other customers.

Security groups

Select security groups

ec2sg sg-046e1598b1b6e9f54 X
VPC-vpc-f8b05f9e

▼ Storage (volumes) [Info](#)

Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp2))
AMI Volumes are not included in the template unless modified

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

Add new volume

Nitro Enclaves are not compatible with instance types that have fewer than 2 vCPUs.

License configurations [Info](#)

Select a license configuration

Metadata accessible [Info](#)

Don't include in launch template

Metadata version [Info](#)

Don't include in launch template

Metadata response hop limit [Info](#)

Don't include in launch template

User data [Info](#)

```
sudo su
yum update -y
yum install httpd -y
systemctl enable httpd.service
cd /var/www/html
aws s3 sync s3://testwebsiteec2s3 /var/www/html
systemctl start httpd.service
```

☐ User data has already been base64 encoded

Cancel

Create launch template

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Choose launch template or configuration [Info](#)

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name

Enter a name to identify the group

demoASG

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

[Switch to launch configuration](#)

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

demoTemplate

Create a launch template [Info](#)

Version

(Default 1)

Create a launch template version [Info](#)

Description	Launch template	Instance type
template:demo	demoTemplate Info	s2.micro
AMI ID	ami-041b6236ad8f2267c	Request Spot instances
Key pair name	ec2sshkeypair	No
Additional details		
Storage (volumes)	-	
Date created		
Fri Oct 15 2021 23:33:56 GMT+0530 (India Standard Time)		

Cancel

Next

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Configure settings

Configure the settings below. Depending on whether you chose a launch template, these settings may include options to help you make optimal use of EC2 resources.

Instance purchase options

Use the launch template to create a uniform configuration among all of the instances in the group. Or, define options to accommodate a wide variety of requirements, such as launching Spot and On-Demand instances.

☒ Adhere to launch template
The launch template determines the purchase option (On-Demand or Spot) and instance type.

☐ Combine purchase options and instance types
Specify how much On-Demand and Spot capacity to launch and multiple instance types (optional). This choice is most helpful for optimizing the scale and cost for a fleet of instances.

Network

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Use:

ap-ADDS2796

112.31.0.0/16

Default

Create a VPC

Subnets

Select subnets

ap-south-1a | subnet-6574813e

112.31.16.0/20

Default

ap-south-1b | subnet-Q29w4e4e

112.31.48.0/20

Default

ap-south-1c | subnet-df1e1286

112.31.16.0/20

Default

Create a subnet

Cancel

Previous

Skip to review

Next

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Configure advanced options

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

Load balancing - optional

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☐ No load balancer
Traffic to your Auto Scaling group will not be forwarded by a load balancer.

☒ Attach to an existing load balancer
Choose from your existing load balancers.

☐ Attach to a new load balancer
Quickly create a load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups
This option allows you to attach Applications, Network, or Gateway Load Balancers.

☐ Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

demoTargetGroup | HTTP

Application Load Balancer

demoTargetGroup | HTTP

Application Load Balancer

demoTargetGroup | HTTP

Application Load Balancer

Health checks - optional

Health-check type

EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

EC2

☒ ELB

Health-check grace period

The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are put into service.

300

 seconds

Additional settings - optional

Cancel

Previous

Skip to review

Next

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Configure group size and scaling policies

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

2

Minimum capacity

1

Maximum capacity

3

2

Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand.

☐ Target tracking scaling policy
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

☒ None

Instance scale-in protection - optional

Instance scale-in protection

If protect from scale-in is enabled, newly launched instances will be protected from scale-in by default.

☐ Disable instance scale-in protection

Cancel

Previous

Skip to review

Next

