

Little bit Advanced

Q1. EC2 with ELB and ASG

Objective: Learn how to create a scalable and highly available web application environment using Amazon EC2 instances, ELB, and ASG.

Approach:

1. Launch EC2 Instances: Start by launching two or more EC2 instances. These instances will run a simple web application (e.g., a "Hello World" page or any basic web service).
2. Configure Load Balancer: Set up an Elastic Load Balancer (ELB) to distribute incoming web traffic across your EC2 instances. This step ensures high availability and fault tolerance.
3. Set Up Auto Scaling Group (ASG): Create an ASG that uses the launched EC2 instances. Configure ASG policies to automatically scale the number of instances up or down based on criteria like CPU usage or network traffic.
4. Test Your Setup: Simulate traffic to test the scaling policies and the load balancer. Observe how ASG adds or removes instances and how ELB distributes traffic.
5. Verify Website Functionality: Ensure that the website hosted on EC2 instances remains accessible and functional during scaling operations.

Goal: By the end of this lab, students will have a hands-on understanding of setting up a load-balanced and auto-scaled web application using AWS services.

The screenshot shows the AWS EC2 Security Groups console. On the left, a sidebar navigation includes: EC2 Dashboard, EC2 Global View, Events, Console-to-Code (Preview), Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations (New), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main content area displays the details for a security group named 'sg-03fccd29d1bbc019b - internet-access'. The 'Details' section shows the security group name, ID, description ('internet accessing'), and VPC ID. The 'Inbound rules' tab is active, showing one rule: 'sg-0837cc9f219bce417' (Security group rule ID), IPv4, HTTP, TCP, and port 80. There are tabs for 'Outbound rules' and 'Tags'.

Creating security group for connecting with SSH

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

[Preview](#)

Instances

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- [New](#)

Images

- AMIs
- AMI Catalog

Elastic Block Store

- Volumes
- Snapshots

Amazon Machine Images

EC2 > Security Groups > sg-067ca4dfa32989a68 - developer_shh_access

sg-067ca4dfa32989a68 - developer_shh_access

[Actions ▾](#)

Details

Security group name	sg-067ca4dfa32989a68	Security group ID	sg-067ca4dfa32989a68	Description	developers ssh access	VPC ID	vpc-0f978c8c6a4569c6f
Owner	462972487428	Inbound rules count	1 Permission entry	Outbound rules count	1 Permission entry		

[Inbound rules](#) [Outbound rules](#) [Tags](#)

Inbound rules (1/1)

group rule...	IP version	Type	Protocol	Port range	Source	Dest
1568d4fe6209a	IPv4	SSH	TCP	22	14.143.137.29/32	-

Creating EC2 instance

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: hello_page [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.

[Search our full catalog including 1000s of application and OS images](#)

Quick Start

Amazon Linux **aws** macOS Ubuntu Windows Red Hat SUSE Li [Browse more AMIs](#) Including AMIs from

Summary

Number of instances [Info](#): 1

Software Image (AMI): [Amazon Linux 2023 AMI 2023.3.2...read more](#) ami-0440d3b780d96b29d

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

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 IOPS, 1 GB of snapshots, and 500 CPU credits available in the month.

[Cancel](#) **Launch Instance** [Review commands](#)

Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro	Family: t2 - 1 vCPU, 1 GiB Memory Current generation: true	Free tier eligible
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: 0.0116 USD per Hour		
On-Demand Linux base pricing: 0.0116 USD per Hour		

Additional costs apply for AMIs with pre-installed software

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

[Create new key pair](#)

Software Image (AMI)
Amazon Linux 2023.5.2... [read more](#)
ami-0440d3b780d96b29d

Virtual server type (instance type)
t2.micro

Firewall (security group)
2 security groups

Storage (volumes)
1 volume(s) - 8 GiB

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 GiB of snapshots, and 100 GiB of bandwidth to the internet.

[Cancel](#) [Launch Instance](#)

Network settings [Info](#)

Network [Info](#)
vpc-0f978c8c6a4569c6f

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](#)

Common security groups [Info](#)

Select security groups

developer_shh_access_sg-067ca4dfa32989a68 X
VPC: vpc-0f978c8c6a4569c6f

internet-access_sg-03fccd29d1bbc019b X
VPC: vpc-0f978c8c6a4569c6f

[Compare security group rules](#)

[Hide all selected](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023.5.2... [read more](#)
ami-0440d3b780d96b29d

Virtual server type (instance type)
t2.micro

Firewall (security group)
2 security groups

Storage (volumes)
1 volume(s) - 8 GiB

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 GiB of snapshots, and 100 GiB of bandwidth to the internet.

EC2 Dashboard

Instances

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances

Instances (1/1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

Instance ID: i-029613911894a2b04 [X](#) [Clear filters](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic
hello_page	i-029613911894a2b04	Running @ Q	t2.micro	Initializing View alarms +		us-east-1c	ec2-54-226-222-110.co...	54.226.222.110	-

Connecting EC2 instance with SSH

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-31-102 ~]$ sudo su
[root@ip-172-31-31-102 ec2-user]# yum update -y
Last metadata expiration check: 0:10:36 ago on Thu Feb 22 06:04:12 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-31-102 ec2-user]# yum install httpd
Last metadata expiration check: 0:10:53 ago on Thu Feb 22 06:04:12 2024.
Dependencies resolved.
=====
Repository           Size
=====
httpd               x86_64      2.4.58-1.amzn2023
=====
Installing:
=====
httpd               x86_64      2.4.58-1.amzn2023
=====
amazonlinux          47 k
=====
Installing dependencies:
=====
apr                 x86_64      1.7.2-2.amzn2023.0.2
amazonlinux          129 k
apr-util             x86_64      1.6.3-1.amzn2023.0.1
amazonlinux          98 k
generic-logos-httpd noarch     18.0.0-12.amzn2023.0.3
amazonlinux          19 k
httpd-core           x86_64      2.4.58-1.amzn2023
amazonlinux          1.4 M
httpd-filesystem     noarch     2.4.58-1.amzn2023
amazonlinux          14 k
httpd-tools           x86_64      2.4.58-1.amzn2023
amazonlinux          81 k
libbrotli            x86_64      1.0.0-4.amzn2023.0.2
amazonlinux          315 k
mailcap              noarch     2.1.49-3.amzn2023.0.3
amazonlinux          33 k
=====
Calling weak dependencies:
=====
apr-util-openssl    x86_64      1.6.3-1.amzn2023.0.1
amazonlinux          17 k
mod_http2            x86_64      2.0.11-2.amzn2023
amazonlinux          150 k
mod_lua               x86_64      2.4.58-1.amzn2023
amazonlinux          61 k
=====
Transaction Summary
=====
Install 12 Packages
=====
Total download size: 2.3 M
Installed size: 6.9 M
Is this ok [y/N]: y
```

```
Complete!
[root@ip-172-31-31-102 ec2-user]# systemctl start httpd
[root@ip-172-31-31-102 ec2-user]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service.
[root@ip-172-31-31-102 ec2-user]# chown -R $USER /var/www/html
[root@ip-172-31-31-102 ec2-user]# echo "<h1>Hello World</h1>" > /var/www/html/hello.html
[root@ip-172-31-31-102 ec2-user]#
```

Opening web page with Public-IP



Hii guys

i am sahil bhandigare....



Creating target group before load balancer to allocate EC2 as a target

EC2 > Target groups > Create target group

Step 1: Specify group details

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

Step 2: Register targets

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.

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.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

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:

Target group name
demo-test

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

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP **80**
1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

IPv4
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

vpc-0f97bc0ca4569c6f
IPv4: 172.31.0.0/16

Protocol version

HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol
 HTTP

Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.
/

Up to 1024 characters allowed.

► Advanced health check settings

Attributes

Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

► Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel **Next**

[EC2](#) > [Target groups](#) > Create target group

Step 1: [Specify group details](#)

Step 2: [Register targets](#)

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (1)									
Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time		
i-029b13911894a2b04	hello_page	Running	developer_shh_access, internet-access	us-east-1c	172.31.31.102	subnet-0770891fe3e839517	February 22, 2024, 11:33 (UTC+0...)		

Selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
T-45555 (separate multiple ports with commas)

[Include as pending below](#)

1 selection is now pending below. Include more or register targets when ready.

Review targets

Targets (1)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time		
i-029b13911894a2b04	hello_page	80	Running	developer_shh_access, internet-access	us-east-1c	172.31.31.102	subnet-0770891fe3e839517	February 22, 2024, 11:33 (UTC+0:00)		

1 pending

[Cancel](#) [Previous](#) [Create target group](#)

[EC2 Dashboard](#) [EC2 Global View](#)

Events

Console-to-Code [Preview](#)

- Instances
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Saving Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations [New](#)
- Images
 - AMIs
 - AMI Catalog
- Elastic Block Store
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs
 - Network Interfaces
- Load Balancing
 - Load Balancers
 - Target Groups
 - Trust Stores [New](#)
- Auto Scaling
 - Auto Scaling Groups

Successfully created the target group: demo-test. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.

[EC2](#) > [Target groups](#) > demo-test

demo-test

Introducing Automatic Target Weights (ATW) to increase application availability
Automatic Target Weights is achieved by turning on anomaly mitigation, which provides responsive, dynamic distribution of traffic to targets based on anomaly detection results. All HTTP/HTTPS target groups now include anomaly detection by default. [Learn more](#)

Details
[arn:aws:elasticloadbalancing:us-east-1:462972487428:targetgroup/demo-test/271dbd19e11818](#)

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-0f978b5a4569cf
IP address type	IPv4		
	Load balancer None associated		

1 Total targets

Health	Unhealthy	Unused	Initial	Draining
0 Healthy	0 Unhealthy	1 Unused	0 Initial	0 Draining
0 Anomalous				

Distribution of targets by Availability Zone (AZ)
Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets [Monitoring](#) [Health checks](#) [Attributes](#) [Tags](#)

Registered targets (1/1) info

Target group route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Instance ID	Name	Port	Zone	Health status	Launch...	Anomaly detection result
i-029b13911894a2b04	hello_page	80	us-east-1c	Unused	Target group is not co...	February ... Normal

[Anomaly mitigation: Not applicable](#) [Deregister](#) [Register targets](#)

Creating application load balancer

EC2 > Load balancers > Create Application 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 can't be changed after the load balancer is created.

Scheme Info
Scheme can't 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 or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

- vpc-0f978bc6a4569cf
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.

us-east-1a (use1-az1)
Subnet

IPv4 address
Assigned by AWS

us-east-1b (use1-az2)
Subnet

IPv4 address
Assigned by AWS

us-east-1c (use1-az4)
Subnet

IPv4 address
Assigned by AWS

us-east-1d (use1-az6)
Subnet

Creating security group

The screenshot shows the AWS Security Groups configuration page. At the top, there is a header with the title "Security groups" and a "Info" link. Below the header, a note states: "A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group." A dropdown menu titled "Select up to 5 security groups" contains one item: "default" (sg-01776e0911b10d519 VPC: vpc-0f978c8c6a4569c6f). There is a "Create new security group" button.

Below the dropdown, the "Listeners and routing" section is visible. It includes a note: "A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets." Under the "Listener HTTP:80" section, there is a table:

Protocol	Port	Default action	Info
HTTP	: 80	Forward to	demo-test Target type: Instance, IPv4 HTTP 1-65535

Buttons for "Remove", "Edit", and "Create target group" are present. Below the table, there is a section for "Listener tags - optional" with a note: "Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them." A "Add listener tag" button is available, with a note: "You can add up to 50 more tags." A "Create target group" button is also present. At the bottom of the page, there is a "Add listener" button.

The screenshot shows the AWS Load Balancers configuration page. At the top, a green success message box says: "Successfully created load balancer: test-demo. It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks." Below the message, the page title is "test-demo".

The main content area is titled "Details". It shows the following information:

Load balancer type	Status	VPC	IP address type
Application	Provisioning	vpc-0f978c8c6a4569c6f	IPv4
Scheme	Internet-facing	Hosted zone Z355XD0TRQ7X7K	Date created February 22, 2024, 12:41 (UTC+05:30)

Below this, there is a "Load balancer ARN" field containing "arn:aws:elasticloadbalancing:us-east-1:462972487428:loadbalancer/app/test-demo/ba671ff355ec846". To the right, there is a "DNS name info" field containing "test-demo-1037404497.us-east-1.elb.amazonaws.com (A Record)".

At the bottom of the page, there are tabs for "Listeners and rules", "Network mapping", "Security", "Monitoring", "Integrations", "Attributes", and "Tags".

Adding security group

The screenshot shows the AWS CloudFormation console with a new stack named 'test-demo'. The 'Details' tab is selected, showing the configuration for a new Application Load Balancer. The 'Security' tab is highlighted with a red circle. In the 'Security groups' section, a new security group named 'internet-access' is listed with the description 'internet accessing'.

Creating another EC2

The screenshot shows the AWS CloudFormation console with a new stack named 'test-demo'. The 'Instances' tab is selected, showing two running EC2 instances: 'hello_page' and 'hello_page2'. The detailed view for 'hello_page2' is shown, including its instance ID, state, type, and network details. The 'Networking' tab is selected in the instance details view.

The screenshot shows the AWS EC2 Target Groups interface. On the left, the navigation menu includes options like EC2 Dashboard, 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, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, and Placement Groups. The main content area displays a success message: "One target registered successfully to demo-test." Below this is a table titled "Target groups (1/1) Info" with one row for "demo-test". The table columns include Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. The "demo-test" row shows "arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/demo-test/123456789012345678" as the ARN, port 80, protocol HTTP, target type Instance, load balancer None associated, and VPC ID vpc-0f978c8c6a4569c6f. A modal window titled "Target group: demo-test" provides detailed information about the target group, including its type (Instance), protocol (HTTP: 80), version (HTTP1), and VPC (vpc-0f978c8c6a4569c6f). It also shows the distribution of targets by Availability Zone (AZ), with 2 healthy targets and 0 unhealthy targets.

Creating image

The screenshot shows the "Create image" interface for instance i-029b13911894a2b04. The top navigation bar includes the AWS logo, Services, Search, and [Alt+S]. The main content area has a title "Create image Info" and a sub-instruction: "An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance." The form fields include:

- Instance ID:** i-029b13911894a2b04 (hello_page)
- Image name:** hello-image (Maximum 127 characters,不可修改)
- Image description - optional:** image for ASG (Maximum 255 characters)
- No reboot:** Enable
- Instance volumes:**

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/...	Create new snapshot fr...	8	EBS General Purpose S...	3000		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Add volume

A note: "During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes."
- Tags - optional:** A note: "A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs." Two radio button options are shown:
 - Tag image and snapshots together: "Tag the image and the snapshots with the same tag."
 - Tag image and snapshots separately: "Tag the image and the snapshots with different tags."
- No tags associated with the resource.**
- Add new tag:** "You can add up to 50 more tags."

At the bottom right are "Cancel" and "Create image" buttons.

Creating Template for ASG

The screenshot shows the 'Create launch template' wizard in the AWS EC2 console. The current step is 'Launch template name and description'. A red circle highlights the 'Launch template name - required' field, which contains 'hello-template'. Below it is a note: 'Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.' The 'Template version description' field contains 'Template for ASG'. Under 'Auto Scaling guidance', there is a checkbox for 'Provide guidance to help me set up a template that I can use with EC2 Auto Scaling'. Below this are sections for 'Template tags' and 'Source template'. To the right, the 'Summary' section shows the selected 'Software Image (AMI)' as 'image for ASG' with ID 'ami-0652ef31d3436fe29'. It also lists 'Virtual server type (instance type)', 'Firewall (security group)', and 'Storage (volumes)'. A callout box provides information about the 'Free tier'. At the bottom are 'Cancel' and 'Create launch template' buttons.

The screenshot shows the 'Application and OS Images (Amazon Machine Image) - required' step. A red circle highlights the 'My AMIs' tab, which is selected. Below it are filters for 'Owned by me' (selected) and 'Shared with me'. The main area displays an 'Amazon Machine Image (AMI)' named 'hello-image' with ID 'ami-0652ef31d3436fe29', created on '2024-02-22T09:47:24.000Z', using 'hvm' virtualization, ENA enabled, and 'ebs' root device type. The 'Description' is 'image for ASG'. The 'Architecture' is 'x86_64' and the 'AMI ID' is 'ami-0652ef31d3436fe29'. To the right, the 'Summary' section is identical to the previous screenshot, showing the same AMI selection and tier information. The 'Create launch template' button is visible at the bottom.

Instance type

t2.micro 1 vCPU | 1 GiB Memory Current generation: true Free tier eligible

All generations Compare instance types

Key pair (login)

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: server1-test

Network settings

Subnet: Don't include in launch template

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups): Select existing security group

Summary

Software Image (AMI): ami-0652ef31d3436fe29

Virtual server type (instance type): t2.micro

Firewall (security group): 2 security groups

Storage (volumes): 1 volume(s) - 8 GiB

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 IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Create launch template

Services

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups): Select existing security group

Security groups: developer_shh_access sg-067ca4dfa32989a68 (VPC: vpc-0f978c8c6a4569c6f), internet-access sg-03fccd29d1bbc019b (VPC: vpc-0f978c8c6a4569c6f)

Storage (volumes)

EBS Volumes

Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3))

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

Add new volume

Summary

Software Image (AMI): ami-0652ef31d3436fe29

Virtual server type (instance type): t2.micro

Firewall (security group): 2 security groups

Storage (volumes): 1 volume(s) - 8 GiB

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 IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Create launch template

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Preview

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

New

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Launch Templates (1/1) [Info](#)

Search

Actions [Create launch template](#)

Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
lt-04ffb85c0f55fe218	hello-template	1	1	2024-02-22T09:54:42.000Z	arn:awssts::462972487428:assumed-role/voclabs/user301...

hello-template (lt-04ffb85c0f55fe218)

Launch template details

Actions [Delete template](#)

Launch template ID lt-04ffb85c0f55fe218	Launch template name hello-template	Default version 1	Owner arn:awssts::462972487428:assumed-role/voclabs/user3011557=amol.kanchar@dctinc.com
--	--	----------------------	--

Details Versions Template tags

Launch template version details

Actions [Delete template version](#)

The screenshot shows the AWS EC2 Launch Templates page. On the left, there's a navigation sidebar with various EC2-related options like Instances, AMIs, and Network & Security. The main area has a title 'Launch Templates (1/1)' with a 'Info' link. Below it is a search bar and a header with 'Actions' and 'Create launch template'. A table lists one launch template: 'lt-04ffb85c0f55fe218' with the name 'hello-template', default version 1, latest version 1, created on 2024-02-22 at 09:54:42.000Z by 'arn:awssts::462972487428:assumed-role/voclabs/user301...'. Below the table, a modal window titled 'hello-template (lt-04ffb85c0f55fe218)' displays 'Launch template details' for the same entry. At the bottom, there's a section for 'Launch template version details' with similar actions.

Creating ASG

The screenshot shows the AWS EC2 Auto Scaling Groups 'Create Auto Scaling group' wizard, Step 1: Choose instance launch options. The left sidebar lists steps from 1 to 7. Step 1 is active, showing 'Choose launch template'. The main area is titled 'Choose instance launch options' with a sub-section 'Instance type requirements'. It shows a launch template 'hello-template' (version Default, ID lt-04ff85c0f55fe218) and an instance type 't2.micro'. A 'Override launch template' button is available. Below this is a 'Network' section with a VPC dropdown set to 'vpc-0f978c8c64a569c6f' (172.31.0.0/16, Default), a 'Create a VPC' button, and a 'Select Availability Zones and subnets' dropdown containing several subnets across different availability zones.

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Instance type requirements Info

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Override launch template

Launch template	Version	Description
hello-template	Default	Template for ASG

Instance type
t2.micro

Network Info

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
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0f978c8c64a569c6f
172.31.0.0/16 Default

Create a VPC

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-east-1e | subnet-0d24ec50e92c78ee4 X
172.31.48.0/20 Default

us-east-1d | subnet-0b3a844a6813779c0 X
172.31.52.0/20 Default

us-east-1c | subnet-0770891fe3e839517 X
172.31.16.0/20 Default

us-east-1b | subnet-0106833ab11e80988 X
172.31.80.0/20 Default

us-east-1a | subnet-0911e170ea031010d X
172.31.0.0/20 Default

us-east-1f | subnet-096eaf4395d1d107 X

AWS Services Search [Alt+S]  

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

Configure advanced options - *optional* Info

Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.

Load balancing Info

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 fronted 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 basic 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 Application, 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  

demo-test | HTTP 
Application Load Balancer: test-demo

AWS Services Search [Alt+S] ☰ 🔍

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

EC2 health checks

Always enabled

Additional health check types - optional | Info

Turn on Elastic Load Balancing health checks | Recommended

Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

ⓘ EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the [Load Balancer console](#)

Turn on VPC Lattice health checks

VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

Health check grace period | Info

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

300 seconds

Additional settings

Monitoring | Info

Enable group metrics collection within CloudWatch

Default instance warmup | Info

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

Enable default instance warmup

aws Services Search [Alt+S] ▾

Step 1 [Choose launch template](#)

Step 2 [Choose instance launch options](#)

Step 3 - optional [Configure advanced options](#)

Step 4 - optional **Configure group size and scaling**

Step 5 - optional [Add notifications](#)

Step 6 - optional [Add tags](#)

Step 7 [Review](#)

Configure group size and scaling - *optional* Info

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▾

Desired capacity
Specify your group size.

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits
Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity	Max desired capacity
<input type="text" value="2"/>	<input type="text" value="5"/> ▾
Equal or less than desired capacity	Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy | [Info](#)
 You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies
 Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy
 Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Metric type | [Info](#)
 Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Target value

Instance warmup | [Info](#)
 seconds

Disable scale in to create only a scale-out policy

Instance maintenance policy - new | [Info](#)
 Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Control availability and cost during replacement events
 An instance maintenance policy determines how much availability your application has when EC2 Auto Scaling replaces instances. It also establishes guardrails that limit the amount of capacity that can be added or removed when replacing instances.

EC2 > Auto Scaling groups

Auto Scaling groups (1/1) | [Info](#)

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
Haloo-ASG	hello-template Version Default	0	Updating capacity...	1	1	5	us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1e...

Auto Scaling group: Haloo-ASG

Group details

Auto Scaling group name Haloo-ASG	Desired capacity 1	Desired capacity type Units (number of instances)	Amazon Resource Name (ARN) arn:aws:autoscaling:us-east-1:462972487428:autoScalingGroup:d0bbccbb0-94f1-4ac2-9ba6-14190e40fa37:autoScalingGroupName/Halloo-ASG
Date created Thu Feb 22 2024 15:37:52 GMT+0530 (India Standard Time)	Minimum capacity 1	Status Updating capacity	
	Maximum capacity 5		

Launch template

Launch template lt-04ff85c0f55fe218 hello-template	AMI ID ami-0652ef31d3436fe29	Instance type t2.micro	Owner arn:aws:sts::462972487428:assumed-role/voclabs/user3011557:amol.kanchan@dictinc.com
Version Default	Security groups -	Security group IDs sg-067ca4dfa32989a68 sg-03fcdd29d1bbc019b	Create time Thu Feb 22 2024 15:24:42 GMT+0530 (India Standard Time)

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

- Instances**
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- New

Images

- AMIs
- AMI Catalog

Elastic Block Store

- Volumes
- Snapshots
- Lifecycle Manager

Network & Security

- Security Groups
- Elastic IPs
- Placement Groups

EC2

Instances (3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
hello_page	i-029b13911894a2b04	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-174-129-122-25.co...	174.129.122.25	-
hello_page2	i-03ddaf4dd6861fee4	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-54-221-151-225.co...	54.221.151.225	-
	i-07c496099abdef6fb	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-18-212-210-40.co...	18.212.210.40	-

Select an instance

EC2

Target groups

Target groups (1/1) Info

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
demo-test	arn:aws:elasticloadbalanci...	80	HTTP	Instance	test-demo	vpc-0f978c8c6a4569c6f

Target group: demo-test

Registered targets (3) Info

Anomaly mitigation: Not applicable

Instance ID	Name	Port	Zone	Health status	Health status details	Launch time	Anomaly detection
i-07c496099abdef6fb	hello_page	80	us-east-1c	Healthy	-	February 22, 2024, 15:37 (U...)	Normal
i-029b13911894a2b04	hello_page	80	us-east-1c	Healthy	-	February 22, 2024, 15:10 (U...)	Normal
i-03ddaf4dd6861fee4	hello_page2	80	us-east-1c	Healthy	-	February 22, 2024, 15:10 (U...)	Normal

Q2. Hosting a Static Portfolio Website on S3

Objective: Learn to host a static website (such as a personal portfolio) on Amazon S3.

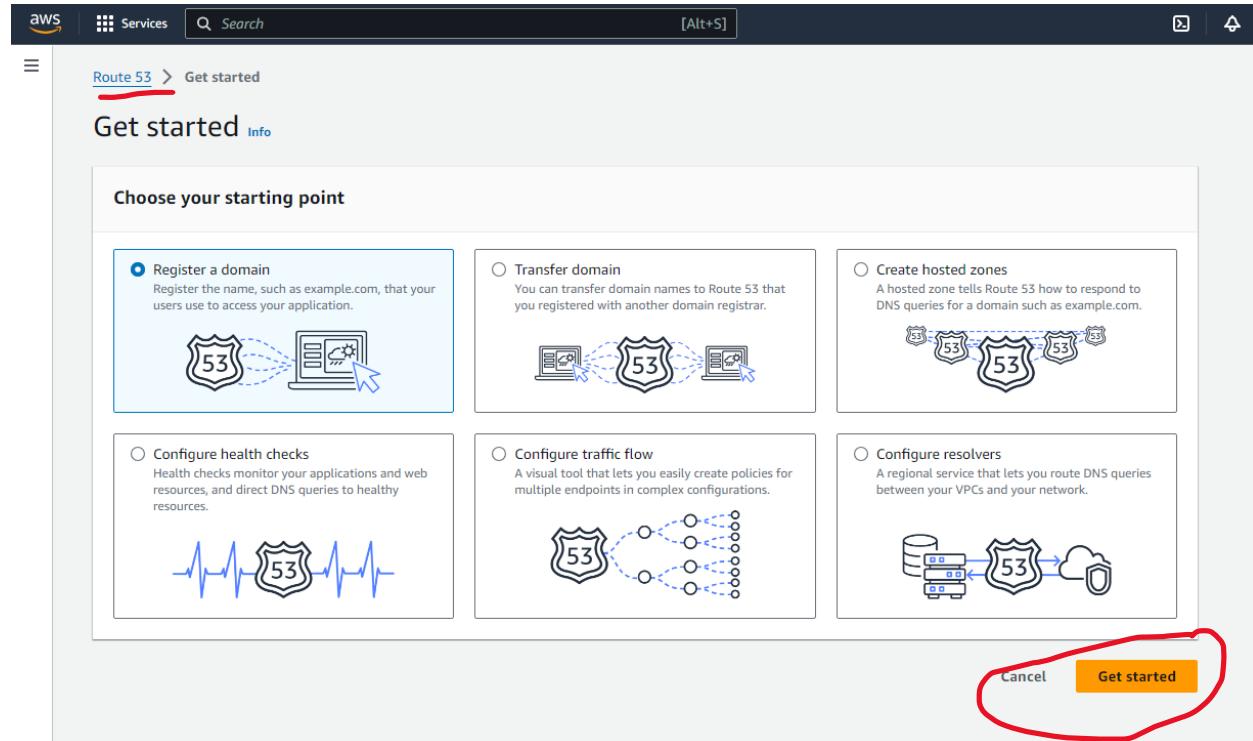
Approach:

1. Create an S3 Bucket: Start by creating a new S3 bucket. Configure the bucket for website hosting, which includes setting permissions to make the content publicly accessible.
2. Upload Website Files: Upload the static files of your portfolio website (HTML, CSS, JavaScript, images) to the S3 bucket.
3. Configure DNS: Use Amazon Route 53 or another DNS service to point a domain name to the S3 bucket. This makes the website accessible via a user-friendly URL.
4. Enable Additional Features (Optional): Implement features like HTTPS for secure access and CloudFront for content delivery optimization.

Goal: Students will understand how to use S3 for hosting static websites, manage bucket permissions, and integrate with other AWS services for a complete web hosting solution.

Steps:

1. To configure DNS we use Amazon Route 53
 - Click on get started in Amazon Route 53



Creating S3 bucket

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

AWS Region: US East (N. Virginia) - us-east-1

Bucket type: 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
Designed for low-latency use cases. These buckets support only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name:

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
 Choose bucket
Format: s3://bucket/prefixes

Access control

Who can access objects in this bucket determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to the 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.

Object ownership

Bucket Versioning

Versions is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Disable
 Enable

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type: Info

Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Disk-tier server-side encryption with AWS Key Management Service keys (DSS-E-KMS)
Select your options with two or more layers of encryption. For details on pricing, see [DSS-E-KMS pricing](#) on the Storage tab of the Amazon S3 pricing page.

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSS-E-KMS. [Learn more](#)

Disable
 Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

☰ ⓘ Successfully created bucket "bucketforstatichosting"
To upload files and folders, or to configure additional bucket settings, choose View details.

View details X ⓘ

Amazon S3 > Buckets

▼ Account snapshot

Last updated: Feb 14, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. [Learn more](#)

Total storage Object count Average object size You can enable advanced metrics in the "default-account-dashboard" configuration.

14.8 KB 1 14.8 KB

General purpose buckets Directory buckets

General purpose buckets (1) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name < 1 > ⓘ

Name	AWS Region	Access	Creation date
bucketforstatichosting	US East (N. Virginia) us-east-1	Objects can be public	February 16, 2024, 15:52:08 (UTC+05:45)

Upload static website

☰ ⓘ

Amazon S3 > Buckets > bucketforstatichosting

bucketforstatichosting [Info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (0) [Info](#) ⌂ Copy S3 URI ⌂ Copy URL ⌂ Download ⌂ Open ⌂ Delete Actions Create folder ⌂ Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix < 1 > ⓘ

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket. Upload				

Amazon S3 > Buckets > bucketforstatichosting > Upload

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, 190.0 B)		
All files and folders in this table will be uploaded.		
<input type="text"/> Find by name		
<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	index.html	-
text/html		

Destination [Info](#)

Destination
s3://bucketforstatichosting

[▶ Destination details](#)

Amazon S3 > Buckets > bucketforstatichosting

bucketforstatichosting [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::bucketforstatichosting	Creation date February 16, 2024, 15:52:08 (UTC+05:45)
---	---	--

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning	Disabled
Multi-factor authentication (MFA) delete	An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled	Edit

CloudShuttle Feedback

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info	Server-side encryption with Amazon S3 managed keys (SSE-S3)
Bucket Key	When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled	Edit

Intelligent-Tiering Archive configurations [\(0\)](#)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

Name	Status	Scope	Days until transition to Archive Access tier	Days until transition to Deep Archive Access tier
No archive configurations	No configurations to display.			
Create configuration				

Server access logging

Log requests for access to your bucket. Use CloudWatch [Logs](#) to check the health of your server access logging. [Learn more](#)

Server access logging	Disabled
Edit	

AWS CloudTrail data events [Info](#)

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

Name	Access
No data events	No data events to display.
Configure in CloudTrail	

Event notifications

Send a notification when specific events occur in your bucket. [Learn more](#)

Name	Event types	Filters	Destination type	Destination
No event notifications	Choose Create event notification to be notified when a specific event occurs.			
Create event notification				

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or see [EventBridge pricing](#)

Send notifications to Amazon EventBridge for all events in this bucket.	Off
Edit	

Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration	Disabled
Edit	

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock	Disabled
Edit	

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays	Disabled
Edit	

Static website hosting

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

Static website hosting	Disabled
Edit	

Amazon S3 > Buckets > bucketforstatichosting > Edit static website hosting

Edit static website hosting [Info](#)

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](#)

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

Error document - optional
This is returned when an error occurs.

Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Cancel [Save changes](#)

Successfully edited bucket policy.

Amazon S3 > Buckets > bucketforstatichosting

bucketforstatichosting Info

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access
Objects can be public

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
⚠ Off
 ▶ Individual Block Public Access settings for this bucket

Edit

cloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preference

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "S3:GetObject",
      "Resource": "arn:aws:s3:::bucketforstatichosting/*"
    }
  ]
}
```

Copy

Object Ownership Info

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.

Object Ownership
Bucket owner enforced
 ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Edit

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Edit

This bucket has the bucket owner enforced setting applied for Object Ownership
 When bucket owner enforced is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 94233cdbeceac0579ac743159d19af80ac7213dd13f5aec7a0fffc5c7b9a639	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Edit

Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. [Learn more](#)

No configurations to display

Copy

Here we see the index file uploaded

The screenshot shows the AWS S3 console interface. At the top, a green header bar displays a success message: "Upload succeeded" with a link to "View details below." Below this, the main title is "Upload: status". A note in a blue box states: "The information below will no longer be available after you navigate away from this page." The main area is titled "Summary". It shows the destination as "s3://bucketforstatichosting" and provides a breakdown of upload results: "Succeeded" (1 file, 190.0 B (100.00%)) and "Failed" (0 files, 0 B (0%)). Below this, there are tabs for "Files and folders" and "Configuration", with "Files and folders" currently selected. The "Files and folders" section shows a single item: "index.html" (1 Total, 190.0 B). A search bar labeled "Find by name" is present. The table below lists the file details:

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	190.0 B	Succeeded	-

Here we can see the website hosted from amazon s3

The screenshot shows a web browser window with the URL <https://bucketforstatichosting.s3.us-east-1.amazonaws.com/index.html?response-content-disposition=inline&X-Amz-Content-Sha256=...>. The page content is "Hii guys" followed by "**i am sahil bhandigare....**".

