

[Guvi Task]

Day 5 - AWS - ELB, ASG, Cloud watch, SNS & SQS

TASK: 1) Create a S3 bucket, with no public access and upload files to the bucket & view the logs for the uploaded files. 2) Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

1) Create a S3 bucket, with no public access and upload files to the bucket & view the logs for the uploaded files.

The screenshot shows the 'Create bucket' page in the AWS S3 console. The 'General configuration' section is active, displaying the AWS Region as 'Asia Pacific (Mumbai) ap-south-1' and a Bucket name field containing 'newapplication-bucket'. Below the name field is a note about uniqueness and naming rules, followed by a 'Choose bucket' button for optional copy settings. The 'Object Ownership' section is also visible, detailing object ownership controls. The bottom navigation bar includes links for CloudShell, Feedback, and various AWS services like Lambda, CloudWatch, and SNS.

The screenshot shows the 'Edit server access logging' page for the 'newapplication-bucket'. The 'Server access logging' section has the 'Enable' option selected. A warning message states that enabling logging will update the bucket policy to include access to the S3 log delivery group. The 'Destination' section specifies a log prefix of 's3://newapplication-bucket/logs'. The bottom navigation bar includes links for CloudShell, Feedback, and various AWS services like Lambda, CloudWatch, and SNS.

AWS Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

Amazon S3

Buckets

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 7

CloudShell Feedback

Objects (986) Info

C 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

Name	Type	Last modified	Size	Storage class
2024-07-07-06-	-	July 7, 2024,		
42-03-	-	12:12:04	494.0 B	Standard
87760842D0DA90DF		(UTC+05:30)		
2024-07-07-06-	-	July 7, 2024,		
42-30-	-	12:12:31	477.0 B	Standard
92B9E22EF848ABE0		(UTC+05:30)		
2024-07-07-06-	-	July 7, 2024,		
42-51-	-	12:12:52	482.0 B	Standard
BB02E66BC855D20D		(UTC+05:30)		
2024-07-07-06-	-	July 7, 2024,		

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

Upload succeeded View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://newapplication-bucket	✓ 31 files, 5.0 MB (100.00%)	0 files, 0 B (0%)

Files and folders Configuration

Files and folders (31 Total, 5.0 MB)

Find by name

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 console. The left sidebar is titled "Amazon S3" and includes sections for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. A "Storage Lens" section is also present. At the bottom of the sidebar, there are links for Feature spotlight, CloudShell, and Feedback.

The main content area shows the path: Amazon S3 > Buckets > newapplication-bucket > 2024-07-07-06-42-03-87760842D0DA90DF. The object name is displayed prominently at the top. Below it are buttons for Copy S3 URI, Download, Open, and Object actions. The "Properties" tab is selected, showing the following details:

Object overview	
Owner 862824dd8a783f86900e503b142eb5247fe282c7cbc95a48141e31b8903fbef0	S3 URI s3://newapplication-bucket/2024-07-07-06-42-03-87760842D0DA90DF
AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3:::newapplication-bucket/2024-07-06-42-03-87760842D0DA90DF
Last modified July 7, 2024, 12:12:04 (UTC+05:30)	Entity tag (Etag) 890164c506b52e6a2cfe910d2a3100bc
Size	

At the bottom right, there are links for Privacy, Terms, and Cookie preferences.

A screenshot of a browser window with several tabs open. The tabs include "Zen Class", "2024-07-07-06-42-03-8776042D0DA90DF", "newapplication-buckets3.ap...", "arn:aws:s3:::newapplication-", "New Tab", and "All Bookmarks". The address bar shows a long URL starting with "newapplication-bucket.s3.ap-south-1.amazonaws.com/2024-07-07-06-42-03-8776042D0DA90DF?response-content-disposition=inline&X-Amz-Security-Toke...". Below the address bar is a toolbar with icons for download, Learn .NET, Bankura STD Code, HP EliteBook 8540p, Access Denied, dell driver download, Online Aws Training, GeeksforGeeks, and All Bookmarks.



2) Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

The screenshot shows the AWS CloudFormation console with a template for launching an EC2 instance. The template includes parameters for Metadata response hop limit (set to 2), Allow tags in metadata (set to Select), and User data (containing a script to install Nginx and set up a basic website). The summary section shows 1 instance being launched with the Canonical AMI, t2.micro instance type, and a new security group. The 'Launch instance' button is highlighted.

Metadata response hop limit | [Info](#)
Allow tags in metadata | [Info](#)
Select
User data - optional | [Info](#)
Upload a file with your user data or enter it in the field.
[Choose file](#)

```
#!/bin/bash
sudo apt update -y
sudo apt install nginx -y
sudo systemctl enable nginx
sudo systemctl start nginx
echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```

Number of instances | [Info](#)
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0c2af51e265bd5e0e
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
[Review commands](#)
[Launch instance](#)

The screenshot shows the AWS CloudFormation console with a template for launching a second EC2 instance. The configuration is identical to the first instance, including the same user data script. The summary section shows 1 instance being launched with the Canonical AMI, t2.micro instance type, and a new security group. The 'Launch instance' button is highlighted.

Allow tags in metadata | [Info](#)
Select
User data - optional | [Info](#)
Upload a file with your user data or enter it in the field.
[Choose file](#)

```
#!/bin/bash
sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2
```

Number of instances | [Info](#)
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0c2af51e265bd5e0e
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
[Review commands](#)
[Launch instance](#)

User data has already been base64 encoded

aws Services Search [Alt+S] Mumbai Sumit_aws_11

EC2 > Security Groups > sg-0adaaad95b0ca378e - launch-wizard-9 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules <small>Info</small>					
Security group rule ID	Type <small>Info</small>	Protocol	Port range	Source <small>Info</small>	Description - optional <small>Info</small>
	<small>Info</small>	<small>Info</small>		<small>Info</small>	
sgr-057a9456f8561c63e	SSH ▾	TCP	22	Cust... ▾	<input type="text"/> 0.0.0.0/0 X
-	Custom TCP ▾	TCP	80	Any... ▾	<input type="text"/> 0.0.0.0/0 X

[Add rule](#)

aws Services Search [Alt+S] Mumbai Sumit_aws_11

EC2 > Security Groups > sg-032be39458a86cf7f - launch-wizard-10 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules <small>Info</small>					
Security group rule ID	Type <small>Info</small>	Protocol	Port range	Source <small>Info</small>	Description - optional <small>Info</small>
	<small>Info</small>	<small>Info</small>		<small>Info</small>	
sgr-0edd0cac1f8e7e7be	SSH ▾	TCP	22	Cust... ▾	<input type="text"/> 0.0.0.0/0 X
-	Custom TCP ▾	TCP	80	Any... ▾	<input type="text"/> 0.0.0.0/0 X

[Add rule](#)

AWS Services Search [Alt+S] Mumbai Sumit_aws_11

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

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

IPv4 VPC CIDR: 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.

ap-south-1a (aps1-az1)
Subnet

IPv4 address
Assigned by AWS

ap-south-1b (aps1-az3)
Subnet

IPv4 address
Assigned by AWS

ap-south-1c (aps1-az2)
Subnet

IPv4 address
Assigned by AWS

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

[EC2](#) > [Security Groups](#) > Create security group

Create security group Info

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 Info

Name cannot be edited after creation.

Description Info

VPC Info

 ▾

Inbound rules Info

The screenshot shows the AWS EC2 Dashboard with the 'Security Groups' section selected. A green success message at the top states: "Security group (sg-0a379f4ba59578a03 | myvpc-sg) was created successfully". Below this, the breadcrumb navigation shows: EC2 > Security Groups > sg-0a379f4ba59578a03 - myvpc-sg. The main title is "sg-0a379f4ba59578a03 - myvpc-sg". On the right, there is an "Actions" dropdown menu. The "Details" tab is selected, displaying the following information:

Security group name	Security group ID	Description	VPC ID
myvpc-sg	sg-0a379f4ba59578a03	Allow port 80	vpc-02d0d84c701781f04

Below this, under the "Owner" section, it shows "730335346690" and "1 Permission entry". Under "Inbound rules count" and "Outbound rules count", it also shows "1 Permission entry". At the bottom, there are tabs for "Inbound rules" (which is active), "Outbound rules", and "Tags".

AWS Services Search [Alt+S] Mumbai Sumit_aws_11 ▾

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](#).

Security groups
Select up to 5 security groups

myvpc-sg X sg-0a379f4ba59578a03 VPC: vpc-02d0d84c701781f04

Listeners and routing [Info](#)

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.

▼ Listener HTTP:80 Remove

Protocol Port Default action [Info](#)

HTTP : 80 Forward to [Select a target group](#) Create target group

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search [Alt+S] Mumbai Sumit_aws_11 ▾

Target group name myvpc-tg

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-02d0d84c701781f04
IPv4 VPC CIDR: 172.31.0.0/16

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

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 (2/2)

Instance ID	Name	State	Security groups
i-0cbfe04b5f7a09425	vpc-webapp2	Running	launch-wizard-10
i-0d8bd05fc0b59594	vpc-webapp1	Running	launch-wizard-9

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

80
1-65535 (separate multiple ports with commas)
Include as pending below

2 selections are now pending below. Include more or register targets when ready.

Review targets

Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IP
i-0cbfe04b5f7a09425	vpc-webapp2	80	Running	launch-wizard-10	ap-south-1a	172.31.32
i-0d8bd05fc0b59594	vpc-webapp1	80	Running	launch-wizard-9	ap-south-1a	172.31.47

2 pending

Cancel Previous Create target group

aws Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

EC2 Dashboard EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs AMI Catalog Elastic Block Store Volumes

EC2 Target groups myvpc-tg

myvpc-tg Actions ▾

Details

arn:aws:elasticloadbalancing:ap-south-1:730335346690:targetgroup/myvpc-tg/2ed5ec694325a159

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-02d0d84c701781f04
IP address type IPv4	Load balancer None associated		
2 Total targets	0 Healthy	0 Unhealthy	2 Unused
	0 Anomalous		0 Initial
			0 Draining

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

Listener HTTP:80

Protocol : Port Default action Info
HTTP : 80 Forward to myvpc-tg
1-65535 Target type: Instance, IPv4
[Create target group](#)

Remove

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

Add listener tag
You can add up to 50 more tags.

Add listener

Load balancer tags - optional
Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

aws Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

EC2 Dashboard X EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs AMI Catalog Elastic Block Store Volumes

Successfully created load balancer: myvpclb
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.

EC2 > Load balancers > myvpclb

myvpclb

Actions

▼ Details

Load balancer type	Status	VPC	Load balancer IP address type
Application	Provisioning	vpc-02d0d84c701781f04	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	ZP97RAFLXTNZK	subnet-05d6b64ddbfe31f69 ap-south-1c (aps1-az2)	July 6, 2024, 12:35 (UTC+05:30)
		subnet-0afb48027e93a61aa ap-south-1a (aps1-az1)	
		subnet-0cfb473bb89283324 ap-	

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S] Mumbai ▾ Sumit_aws_11 ▾

EC2 Dashboard X EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs AMI Catalog Elastic Block Store Volumes

Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers < 1 > ⚙️

Name	DNS name	State	VPC ID	Availability Zones
myvpclb	myvpclb-761456383.ap-s...	Active	vpc-02d0d84c701781f...	3 Availability Zones

Load balancer: myvpclb

Details | Listeners and rules | Network mapping | Resource map - new | Security | Monitoring | Integrations

Details

Load balancer type	Status	VPC	Load balancer IP address type
Application	Active	vpc-02d0d84c701781f04	IPv4

