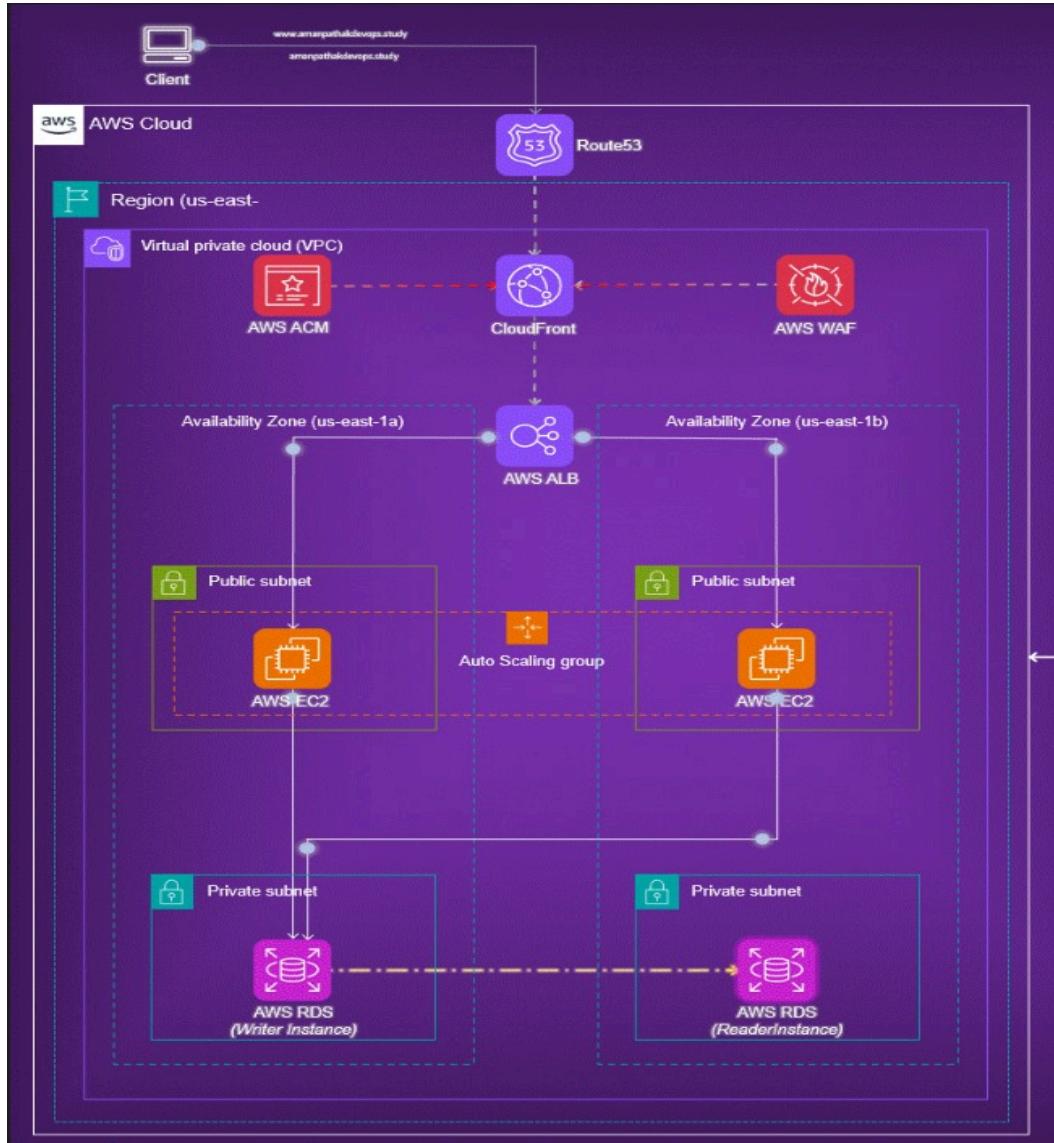


Creating 2 Tiered Architecture in AWS



1) Create one vpc name=challa-vpc

Your VPCs (2) Info						
<input type="checkbox"/> Name		VPC ID	State	IPv4 CIDR	IPv6 CIDR	Actions Create VPC
<input type="checkbox"/>	-	vpc-0dc954a8e763520b0	Available	172.31.0.0/16	-	dopt-01cc
<input type="checkbox"/>	challa-vpc	vpc-039c68c69436ba849	Available	10.0.0.0/16	-	dopt-01cc

- 2) Create 2 public subnets in 1a and 1b availability zone for ec2 server and 3 private subnets for rds in 1a and 1b and 1c availability zones

Subnets (8) Info					
Last updated less than a minute ago C Actions Create subnet					
	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	-	subnet-0201cee82b4b92500	Available	vpc-0dc954a8e763520b0	172.31.0.0/20
<input type="checkbox"/>	-	subnet-049d8679363acd1ce	Available	vpc-0dc954a8e763520b0	172.31.16.0/20
<input type="checkbox"/>	challa-sub1-pub	subnet-00666c99fd2eac620	Available	vpc-039c68c69436ba849 challa-vpc	10.0.0.0/24
<input type="checkbox"/>	challa-sub2-pub	subnet-060d4e0a8e502e042	Available	vpc-039c68c69436ba849 challa-vpc	10.0.1.0/24
<input type="checkbox"/>	challa-sub3-private	subnet-0b17aec0ee07406ec	Available	vpc-039c68c69436ba849 challa-vpc	10.0.20.0/24
<input type="checkbox"/>	challa-sub4-private	subnet-0e566310386985fb2	Available	vpc-039c68c69436ba849 challa-vpc	10.0.10.0/24
<input type="checkbox"/>	challa-sub5-private	subnet-01221b6c91a32845a	Available	vpc-039c68c69436ba849 challa-vpc	10.0.2.0/24

- 3) Now go to 2 public subnets click action edit subnet setting click on enable Enable auto-assign public IPv4 address

VPC > Subnets > [subnet-00666c99fd2eac620](#) > Edit subnet settings

Edit subnet settings [Info](#)

Subnet
Subnet ID: subnet-00666c99fd2eac620 Name: challa-sub1-pub

Auto-assign IP settings Info
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.
<input checked="" type="checkbox"/> Enable auto-assign public IPv4 address Info
<input type="checkbox"/> Enable auto-assign customer-owned IPv4 address Info Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.
<input type="checkbox"/> Enable resource name DNS A record on launch Info
<input type="checkbox"/> Enable resource name DNS AAAA record on launch Info
Hostname type Info <input type="radio"/> Resource name <input checked="" type="radio"/> IP name

- 4) Create challa-igw and attach to challa-vpc

Internet gateways (2) Info					
Search Actions Create internet gateway					
	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-03fa492fa7003b207	Attached	vpc-0dc954a8e763520b0	058264331590
<input type="checkbox"/>	challa-igw	igw-01ca7646899d78c09	Attached	vpc-039c68c69436ba849 challa-vpc	058264331590

- 5) Now create 2 route tables one is for public subnets and another one is private subnets
6) And route igw and subnet association

Route tables (4) Info						
		Last updated less than a minute ago	Actions	Create route table		
<input type="checkbox"/> Name		Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-08b0525906d1551ab	-	-	Yes	vpc-0dc954a8e763520b0
<input type="checkbox"/>	-	rtb-09d1ac7028bf34630	-	-	Yes	vpc-039c68c69436ba849
<input type="checkbox"/>	challa-route1-pub	rtb-0577258f4cf08f4c0	2 subnets	-	No	vpc-039c68c69436ba849
<input type="checkbox"/>	challa-route2-private	rtb-05427d9a7ee6dad4b	3 subnets	-	No	vpc-039c68c69436ba849

7) Create security group name =challa-sg allow ssh and http and mysql add port numbers 443, 80,3306,22

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
SSH	TCP	22	Anyw... Info	<input type="text" value="0.0.0.0/0"/> Delete
HTTP	TCP	80	Anyw... Info	<input type="text" value="0.0.0.0/0"/> Delete
MYSQL/Aurora	TCP	3306	Anyw... Info	<input type="text" value="0.0.0.0/0"/> Delete
				<input type="text" value="0.0.0.0/0"/> Delete

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Security Groups (3) Info				
Actions Export security groups to CSV Create security group				
<input type="checkbox"/> Find resources by attribute or tag				
<input type="checkbox"/> Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	sg-017383c390e4e5a08	default	vpc-0dc954a8e763520b0	default VPC s
<input type="checkbox"/>	sg-02235dfa9c17f4a5	default	vpc-039c68c69436ba849	default VPC s
<input type="checkbox"/>	sg-08bdfbe23c85cbe54	challa-sg	vpc-039c68c69436ba849	allow

8) Now launch ec2 instance 2 using public subnet

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more
ami-04408457f9fa03be3

Virtual server type (instance type): t2.micro

Firewall (security group): challa-sg

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, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Launch instance

9) Same way launch 2 instances name rao

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...read more
ami-04408457f9fa03be3

Virtual server type (instance type): t2.micro

Firewall (security group): challa-sg

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, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Launch instance

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
rao	i-07ab0b29c6780e3d3	Running	t2.micro	Initializing	View alarms	ap-south-1b	-
challa	i-0261705bc73964bed	Running	t2.micro	Initializing	View alarms	ap-south-1a	-

10) Now connect challa and install nginx

11) Using #sudo -i

```
12) #yum update  
13) #yum install nginx -y  
14) #cd /usr/share/nginx/html  
15) #rm -f index.html  
16) #vi index.html (hi this is challa save and exit)  
17) #systemctl restart nginx
```

```
[root@ip-10-0-0-138 html]# history  
1 yum update  
2 yum install nginx  
3 cd /usr/share/nginx/html/  
4 rm -f index.html  
5 vi index.html  
6 systemctl restart nginx  
7 clear  
8 history  
[root@ip-10-0-0-138 html]# |
```

18) Now copy challa server public ip paste in google



19) Now connect rao server do same above steps
20) And copy public ip paste in google



hi this is rao

21) Now create target group name challa-tg
22) Chose instance target type= instances
23) Target group name = challa-tg
24) vpc= challa-vpc and click next

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-07ab0b29c6780e3d3	rao	Running	challa-sg
i-0261705bc73964bed	challa	Running	challa-sg

2 selected

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

Include as pending below

Review targets

- 25) Select both rao and challa and click includes as pending below and click create target group

Target groups (1) [Info](#)

Name	ARN	Port	Protocol	Target type	Load balancer
challa-tg	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/challa-tg/53f34567890123456789012345678901	80	HTTP	Instance	None associated

- 26) Now create load balancer andd Select application load balancer

- 27) Load balancer name= challa-loadbalancer

- 28) scheme= internet facing

- 29) vpc= challa-vpc

- 30) Select both availability zones public and select challa-sg

The screenshot shows the AWS VPC Subnets page. It lists three subnets under the ap-south-1a (aps1-az1) availability zone:

- subnet-00666c99fd2eac620 (challa-sub1-pub): IPv4 address assigned by AWS.
- subnet-060d4e0a8e502e042 (challa-sub2-pub): IPv4 address assigned by AWS.
- subnet-060d4e0a8e502e042 (challa-sub3-pub): IPv4 address assigned by AWS.

Below the subnets, there is a section for Security groups with a note: "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 shows "challa-sg" selected.

31) Listener = challa-tg

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.

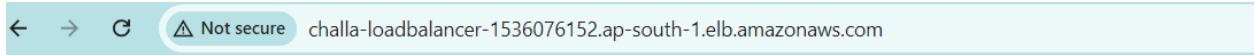
The screenshot shows the AWS Load Balancer Listener configuration page for port 80. The configuration is as follows:

- Protocol: HTTP
- Port: 80
- Default action: Forward to **challa-tg** (Target type: Instance, IPv4)
- Listener tags - optional: Add listener tag (You can add up to 50 more tags.)

32) Copy challa load balancer dns name paste google do refresh check

The screenshot shows a browser window with the URL challa-loadbalancer-1536076152.ap-south-1.elb.amazonaws.com. The status bar indicates "Not secure".

hi this is rao



hi this is challa

- 33) Now create ami using challa instance
- 34) Select challa instance click actions click create image and template and click create image
- 35) Image name= challa-ami
- 36) Enable no reboot
- 37) Create image

Amazon Machine Images (AMIs) (1/1) Info					
Owned by me		Find AMI by attribute or tag		Actions	
Name	AMI name	AMI ID	Source	Owner	Visit
<input checked="" type="checkbox"/> challa-ami	challa-ami	ami-0d847c3072bf7fa40	058264331590/challa-ami	058264331590	Private

- 38) Now go to template create templet
- 39) Templet name= challa-temp
- 40) ami= challa-ami
- 41) Instance type =t2.micro
- 42) keypair= challa
- 43) Security group =challa-sg
- 44) Click create launch templet

Launch Templates (1/1) Info						
Actions						
Create launch template						
Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created ...	
<input checked="" type="checkbox"/> lt-020a75bd7694673c7	challa-temp	1	1	2024-08-07T18:12:47.000Z	arn:aws:ia...	

- 45) Now create auto scaling
- 46) name= challa-autosg
- 47) templet= challa-temp
- 48) Select vpc and availability zones

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-039c68c69436ba849 (challa-vpc)
10.0.0.0/16

[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

ap-south-1a | subnet-00666c99fd2eac620 (challa-sub1-pub)
10.0.0.0/24

ap-south-1b | subnet-060d4e0a8e502e042 (challa-sub2-pub)
10.0.1.0/24

[Create a subnet](#)

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

49) Select attach to existing load balancer and select choose from your loadbalancer target group select challa-tg

Load balancing [Info](#) [Alt+S]

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](#)

Load balancing

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

challa-tg | HTTP
Application Load Balancer: challa-loadbalancer

VPC |attice integration options [Info](#)

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

80°F Haze ENG IN 11:45 PM 07-08-2024

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 <input type="text" value="2"/>	Max desired capacity <input type="text" value="3"/>
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.

<input checked="" type="radio"/> No scaling policies Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.	<input type="radio"/> 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.
---	---

- 50) Desired capacity =2
 51) Min desired capacity =2
 52) Max desired capacity =3
 53) Select no auto scaling policy click create autoscaling group

Auto Scaling groups (1/1) Info								
Create Auto Scaling group								
<input type="checkbox"/> Name <input type="checkbox"/> Launch template/configuration <input type="checkbox"/> Instances <input type="checkbox"/> Status <input type="checkbox"/> Desired capacity <input type="checkbox"/> Min <input type="checkbox"/> Max <input type="checkbox"/> Available								
<input checked="" type="checkbox"/> challa-autosg	challa-temp Version Default	0	<input type="checkbox"/> Updating capacity...	2	2	3	ap-south...	

- 54) Go ec2 instances and check new instances create automatically

Instances (4) Info								
<input type="checkbox"/> Find Instance by attribute or tag (case-sensitive)								
<input type="checkbox"/> Instance state = running X <input type="checkbox"/> Clear filters								
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP	
rao	i-07ab0b29c6780e3d3	<input checked="" type="checkbox"/> Running Q Q	t2.micro	<input checked="" type="checkbox"/> 2/2 checks passed	View alarms +	ap-south-1b	-	
i-05fedba99794ca64e	i-05fedba99794ca64e	<input checked="" type="checkbox"/> Running Q Q	t2.nano	<input checked="" type="checkbox"/> Initializing	View alarms +	ap-south-1b	-	
challa	i-0261705bc73964bed	<input checked="" type="checkbox"/> Running Q Q	t2.micro	<input checked="" type="checkbox"/> 2/2 checks passed	View alarms +	ap-south-1a	-	
i-0878ccf7c76b01c0b	i-0878ccf7c76b01c0b	<input checked="" type="checkbox"/> Running Q Q	t2.nano	<input checked="" type="checkbox"/> Initializing	View alarms +	ap-south-1a	-	

- 55) Now go to route 53 create hosted zone
 56) Domain name = give your domain name ex= rajeshweb.online
 57) Select public hosted zones and create hosted zone

Hosted zone configuration

Domain name [Info](#)
This is the name of the domain that you want to route traffic for.

Description - optional [Info](#)
This value lets you distinguish hosted zones that have the same name.

Type [Info](#)
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.
 Public hosted zone
A public hosted zone determines how traffic is routed on the internet.
 Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.

Tags [Info](#)
Apply tags to hosted zones to help organize and identify them.
No tags associated with the resource.
[Add tag](#)
You can add up to 50 more tags.

[Cancel](#) [Create hosted zone](#)

Route 53

Route 53 > Hosted zones > rajeshweb.online

Hosted zone details

[Edit hosted zone](#)

Records (2) [Info](#)

Record ...	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s...)	Health ...
rajeshweb...	NS	Simple	-	No	ns-1444.awsdns-52.org. ns-989.awsdns-59.net. ns-1841.awsdns-38.co.uk. ns-469.awsdns-58.com.	172800	-
rajeshweb...	SOA	Simple	-	No	ns-1444.awsdns-52.org. aw...	900	-

- 58) Go to go-daddy and update name servers there
- 59) Now go to rajeshweb.online next create record turn on alias
- 60) Route traffic = alias to application load balancer
- 61) Region = us-east (N -virginia)
- 62) Select challa load balancer
- 63) Click crete record

Quick create record

[Switch to wizard](#)

Record 1

Record name [Info](#) **subdomain** rajeshweb.online **Record type** [Info](#) A – Routes traffic to an IPv4 address and some AWS resources

Keep blank to create a record for the root domain.

Alias

Route traffic to [Info](#) Alias to Application and Classic Load Balancer

US East (N. Virginia)

Q dualstack.chall-loadbalancer-717484992.us-east-1.elb.amazonaws.com

Alias hosted zone ID: Z355XD0TRQ7X7K

Routing policy [Info](#) Simple routing **Evaluate target health** Yes

64) Now go to google search rejeshweb.online



hi this is challa



hi this is rao

65) Now go acm

66) Select region and click request certificate

Request certificate

Certificate type Info

ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for ACM to provide.

Request a public certificate

Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.

Request a private certificate

No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit

[AWS Private Certificate Authority](#)

Cancel

Next

67) Give fully qualified domain name= rajeshweb.online

68) Validation method = DNs validation

Domain names

Provide one or more domain names for your certificate.

Fully qualified domain name Info

rajeshweb.online

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Validation method Info

Select a method for validating domain ownership.

DNS validation - recommended

Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

Email validation

Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

Key algorithm Info

Select an encryption algorithm. Some algorithms may not be supported by all AWS services.

RSA 2048

RSA is the most widely used key type.

69) Click on request

70) Click create record in route 53

Domains (1)				
Domain	Status	Renewal status	Type	CNAME name
rajeshweb.online	Pending validation	-	CNAME	2acfe254467761823c4257e4fd5609f0.

ⓘ Successfully requested certificate with ID df8a9501-96eb-443c-bc24-a1f66c35f7b9

A certificate request with a status of pending validation has been created. Further action is needed to complete the validation and approval of the certi

AWS Certificate Manager > Certificates > df8a9501-96eb-443c-bc24-a1f66c35f7b9 >
Create DNS records in Amazon Route 53

Create DNS records in Amazon Route 53 (1/1)

Search domains 1 match

Validation status = Pending validation X Validation status = Failed X Is domain in Route 53? = Yes X

Clear filters

< 1 >

<input checked="" type="checkbox"/>	Domain	Validation status	Is domain in Route 53?
<input checked="" type="checkbox"/>	rajeshweb.online	Pending validation	Yes

Cancel

Create records

71) Select rajeshweb.online create record it update CNAME in route 53 record check there

AWS Certificate Manager > Certificates

Certificates (1)

Delete

Manage expiry events

Import

Request

< 1 >

<input type="checkbox"/>	Certificate ID	Domain name	Type	Status	In
<input type="checkbox"/>	84ce86ae-f1ad-4478-ab29-0615ad96aace	rajeshweb.online	Amazon Issued	Issued	Yes

72) Now go to cloud front create a distributions

73) Origin domain = challa-lb (select load balancer)

74) protocol= select http only (mach viewer)

Screenshot of the AWS CloudFront 'Create distribution' wizard, Step 1: Origin.

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name.
 X

Protocol [Info](#)
 HTTP only
 HTTPS only
 Match viewer

HTTP port
Enter your origin's HTTP port. The default is port 80.

HTTPS port
Enter your origin's HTTPS port. The default is port 443.

Minimum Origin SSL protocol
The minimum SSL protocol that CloudFront uses with the origin.
 TLSv1.2
 TLSv1.1

Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.
[Add header](#)

Enable Origin Shield
Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.
 No
 Yes

[► Additional settings](#)

Default cache behavior

Path pattern [Info](#)

75) Viewer protocol policy = redirect toHTTP to HTTPS

Default cache behavior

Path pattern [Info](#)

Default (*)

Compress objects automatically [Info](#)

No
 Yes

Viewer

Viewer protocol policy

HTTP and HTTPS
 Redirect HTTP to HTTPS
 HTTPS only

Allowed HTTP methods

GET, HEAD
 GET, HEAD, OPTIONS
 GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Cache HTTP methods
GET and HEAD methods are cached by default.
 OPTIONS

Restrict viewer access

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

Cache policy and origin request policy (recommended)
 Legacy cache settings

Cache policy
Choose an existing cache policy or create a new one.
 CachingDisabled
Policy with caching disabled
[Create cache policy](#) [View policy](#)

Origin request policy - *optional*
Choose an existing origin request policy or create a new one.
 AllViewer
Recommended for Elastic Load Balancing
Policy to forward all parameters in viewer requests
[Create origin request policy](#) [View policy](#)

Response headers policy - *optional*
Choose an existing response headers policy or create a new one.
 Select response headers
[Create response headers policy](#)

► Additional settings

Web Application Firewall (WAF) [Info](#)

Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

Use monitor mode
Count how many of your requests would be blocked by this WAF configuration. When ready, you can disable monitor mode to begin blocking requests.

Included security protections

- Protect against the most common vulnerabilities found in web applications.
- Protect against malicious actors discovering application vulnerabilities.
- Block IP addresses from potential threats based on Amazon internal threat intelligence

Additional protections for dynamic applications and APIs [Recommended](#)

SQL protections
Block malicious request patterns that attempt to exploit SQL databases, like SQL injection. Recommended for applications that connect to a SQL database.

Rate limiting
Block HTTP flood attacks, also known as Denial of Service (DoS), that can affect availability, compromise security, or consume excessive resources. This rule rate limits requests for a given IP address that exceeds the allowed rate for your application.

Price estimate

76) Settings use all edge locations

77) Alternate domain name click add item = `rajeshweb.online`

78) Custom ssl certificate = Select your acm certificate click create deploying

The screenshot shows the AWS CloudFront 'Settings' page. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, a search bar, and keyboard shortcuts [Alt+S]. Below the navigation is a sidebar with a 'Settings' section. The main content area has several sections:

- Price class:** [Info](#). Choose the price class associated with the maximum price that you want to pay. The selected option is **Use all edge locations (best performance)**.
- Alternate domain name (CNAME) - optional:** Add the custom domain names that you use in URLs for the files served by this distribution. An input field contains `rajeshweb.online`, with a **Remove** button and a **Add item** button below it.
- Custom SSL certificate - optional:** Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1). A dropdown menu shows `rajeshweb.online (dcf8a4b3-5306-4f91-8e86-ac78fa504371)`, and a **Request certificate** button is next to it.
- Legacy clients support - \$600/month prorated charge applies. Most customers do not need this.** CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS. A checkbox labeled **Enabled** is present.
- Security policy:** The security policy determines the SSL or TLS protocol and the specific ciphers that CloudFront uses for HTTPS connections with viewers (clients). A dropdown menu shows `TLSv1.2_2021 (recommended)`.

Supported HTTP versions
Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

HTTP/2
 HTTP/3

Default root object - optional
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

Standard logging
Get logs of viewer requests delivered to an Amazon S3 bucket.

Off
 On

IPv6
 Off
 On

Description - optional

Distributions (1) <small>Info</small>
<input type="text" value="EPXUAAUJUSOB79"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Create distribution"/>
< 1 > ⟳

79) Now go to route 53 and delete load balancer record create new record

80) Turnon alias

81) Select cloudfont distribution

82) Select cloudfont name

Route 53 > Hosted zones > rajeshweb.online > Create record

Create record [Info](#)

Quick create record [Switch to wizard](#)

Record 1

Record name [Info](#): subdomain rajeshweb.online

Record type [Info](#): A – Routes traffic to an IPv4 address and some AWS resources

Keep blank to create a record for the root domain.

Alias

Route traffic to [Info](#): Alias to CloudFront distribution

US East (N. Virginia)

An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).

Choose distribution

rajeshweb.online (d3sjj0vl6aergq.cloudfront.net)

Simple routing No

Add another record

83) Click create record

84) Now go to search with your domain now it show secure way

← → C rajeshweb.online

hi this is rao

85) Now go to rds and crete rds

86)Now go to databases

87)Select standard create select MY SQL

The screenshot shows the AWS RDS console for creating a new database instance. The 'Standard create' option is selected. In the 'Engine options' section, 'MySQL' is chosen. A tooltip for MySQL is displayed on the right, stating: 'MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.' The tooltip also lists several features:

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance Instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

88)Select multi-az-db cluster
89)Db cluster identifier=rao-database

The screenshot shows the continuation of the RDS instance creation process. Under 'Deployment options', 'Multi-AZ DB Cluster' is selected. This creates a cluster with a primary DB instance and two readable standby DB instances in different Availability Zones (AZ). The 'DB cluster identifier' field is filled with 'rao-database'. A tooltip for MySQL is present on the right, reiterating its features and benefits.

90) username= rao
91) Cluster management type= self mange
92) Master password= rao1234

The screenshot shows the AWS RDS console with the URL us-east-2.console.aws.amazon.com/rds/home?region=us-east-2#launch-dbinstance. The page is titled "Launch DB instance" for MySQL. It includes fields for "DB instance identifier" (rao), "Master user password", and "Confirm master password". Below these are sections for "Instance configuration" and "Storage configuration". On the right, a tooltip for "MySQL" lists its features: supports database sizes up to 64 TiB, various instance classes, automated backup, point-in-time recovery, up to 15 read replicas per instance, and cross-region replication.

93) connectivity= connect to an ec2 compute resource

94) Click automatic setup

95) Public access= no

96) Vpc sg=choose exciting

97) Select sg click create database

The screenshot shows the AWS RDS console with the URL us-east-2.console.aws.amazon.com/rds/home?region=us-east-2#launch-dbinstance. The page is titled "Create database - RDS MySQL". It includes fields for "DB subnet group", "Public access", and "VPC security group (firewall)". The "Automatic setup" option is selected for the DB subnet group. The "No" option for public access is selected. The "Choose existing" option is selected for the VPC security group. A tooltip on the right provides information about MySQL features.

Databases (1)

DB identifier	Status	Role	Engine	Region & AZ	Size	Recommendations	CPU
rao-database	Creating	Instance	MySQL Community	us-east-1b	db.t3.micro	-	-

98) Now go to challa instance and install mysql in challa server

99) Use this link to install my sql in amazon linx

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.CreatingConnecting.MySQL.html

100) #sudo dnf update -y

101) #sudo dnf install mariadb105

102) #mysql --version

103) Now go to rao-database click rao and copy writer end point

Endpoints (2)

Endpoint copied	Status	Type	Port
rao-database.cluster-cxs6cq6muyc7.us-east-2.rds.amazonaws.com	Available	Writer	3306
rao-database.cluster-ro-cxs6cq6muyc7.us-east-2.rds.amazonaws.com	Available	Reader	3306

104) Go to terminal

105) #mysql -h paste here endpoint -u username -p click enter and type password now you connect my sql

```

mariadb105-common-3:10.5.25-1.amzn2023.0.1.x86_64
perl-Sys-Hostname-1.23-477.amzn2023.0.6.x86_64
Complete!
[root@ip-10-0-1-58 ~]# mysql --version
mysql  Ver 15.1 Distrib 10.5.25-MariaDB, for Linux (x86_64) using EditLine wrapper
[root@ip-10-0-1-58 ~]# mysql -h rao-database.cneeks86817d.us-east-1.rds.amazonaws.com -u rao -p venkatlovesri
Enter password:
ERROR 1049 (42000): unknown database 'venkatlovesri'.
[root@ip-10-0-1-58 ~]# mysql -h rao-database.cneeks86817d.us-east-1.rds.amazonaws.com -u rao -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 26
Server version: 8.0.35 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MySQL [(none)]>

```

- 106) > show databases;
- 107) > create database rao;
- 108) > show databases;

```

root@ip-10-0-1-58-
MySQL [(none)]> clear
MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| sys            |
+-----+
4 rows in set (0.004 sec)

MySQL [(none)]> create database rao;
Query OK, 1 row affected (0.006 sec)

MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| rao            |
| sys            |
+-----+
5 rows in set (0.001 sec)

```

The screenshot shows a Windows terminal window with a black background. At the top, there's a title bar with the path 'root@ip-10-0-1-58-' and a close button. Below the title bar is a command-line interface for MySQL. The user has run several commands: 'clear' to clear the screen, 'show databases;' to list existing databases (which shows four: 'information_schema', 'mysql', 'performance_schema', and 'sys'), 'create database rao;' to create a new database named 'rao', and finally 'show databases;' again to verify that the new database is listed along with the others. The MySQL prompt 'MySQL [(none)]>' appears at the bottom of the terminal window.