



AWS MASTER FINAL PROJECT



ASTHALOCHAN MOHANTA
MSC DATASCIENCE
22MDSA53

1. CREATE YOUR OWN VPC

The screenshot shows the 'Create VPC' wizard in the AWS VPC Management Console. The 'VPC settings' step is selected. In the 'Resources to create' section, 'VPC only' is chosen. A 'Name tag - optional' field contains 'my-vpc'. Under 'IPv4 CIDR block', 'IPv4 CIDR manual input' is selected, with '10.0.0.0/16' entered. In the 'IPv6 CIDR block' section, 'No IPv6 CIDR block' is selected. The 'Tenancy' dropdown is set to 'Default'. At the bottom, there are 'Next Step' and 'Cancel' buttons.

2. CREATE SUBNET (PRIVATE + PUBLIC) IN OUR OWN VPC

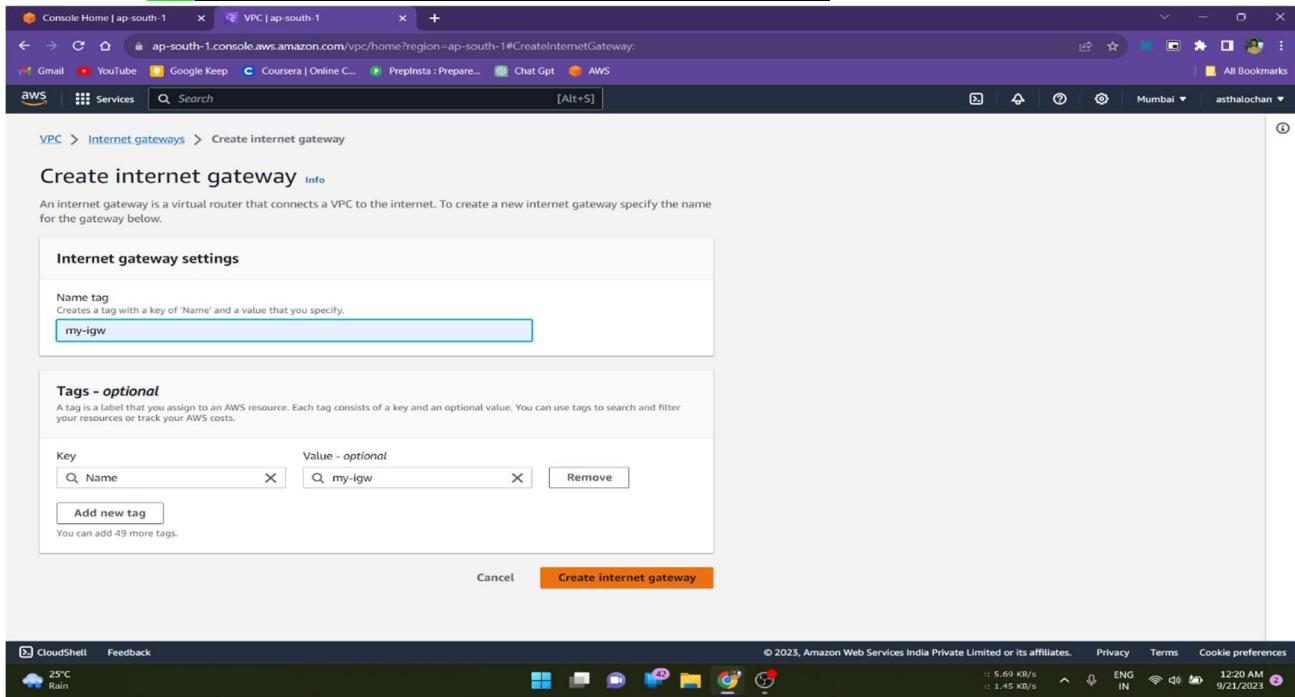
The screenshot shows the 'Create subnet' wizard in the AWS VPC Management Console. In the 'VPC' section, 'vpc-04acc58517024f523 (my-vpc)' is selected. Under 'Associated VPC CIDRs', '10.0.0.0/16' is listed. In the 'Subnet settings' section, 'public-sub-1' is specified as the subnet name and 'Asia Pacific (Mumbai) / ap-south-1' as the availability zone. An 'IPv4 CIDR block' of '10.0.0.0/24' is chosen. At the bottom, there are 'Next Step' and 'Cancel' buttons.

The screenshot shows the 'Subnets' list in the AWS VPC Management Console. It displays two subnets: 'private-sub-1' and 'public-sub-1'. Both subnets are in a 'Available' state, associated with 'vpc-04acc58517024f523 | my-vpc', and have their respective IPv4 CIDRs: '10.0.2.0/24' and '10.0.1.0/24'. The table includes columns for Name, Subnet ID, State, VPC, and IPv4 CIDR.

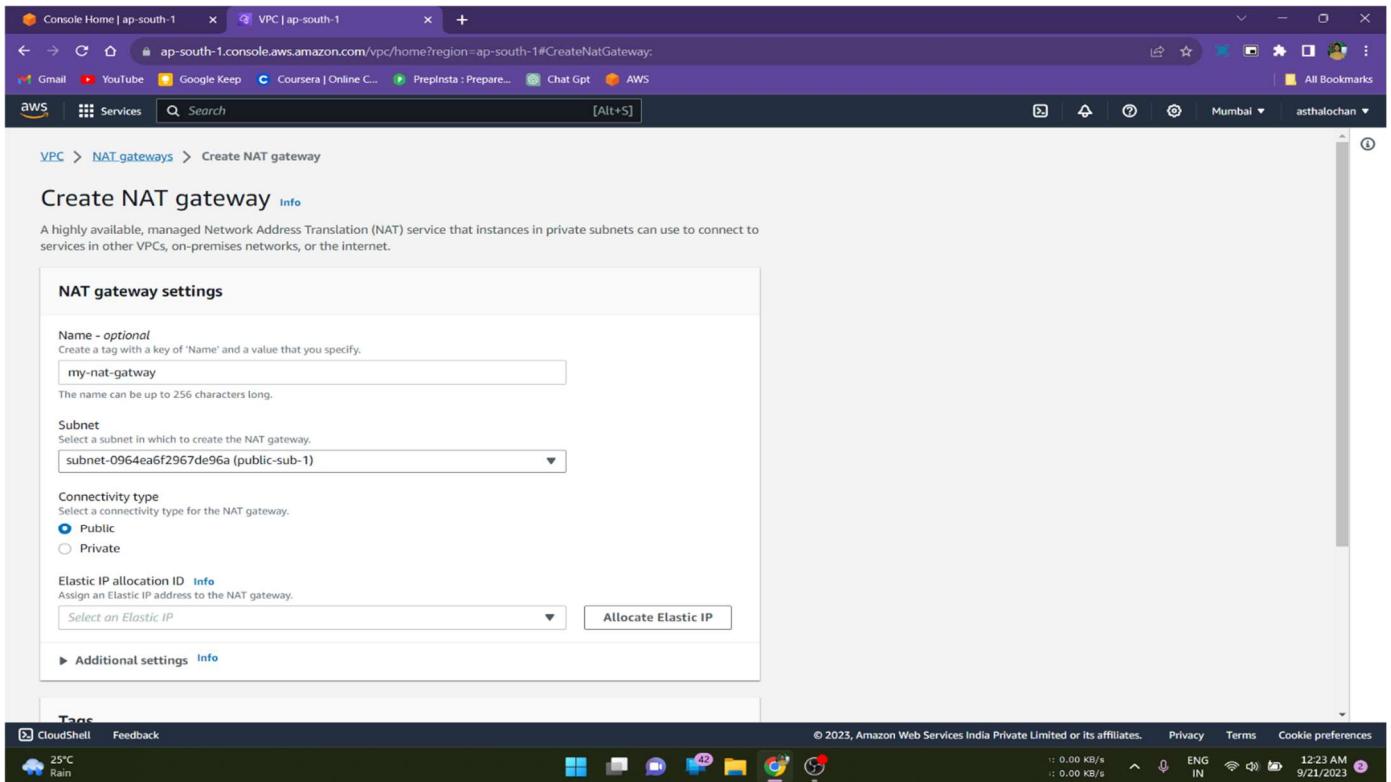
Name	Subnet ID	State	VPC	IPv4 CIDR
private-sub-1	subnet-03bba6282b9abb1fb	Available	vpc-04acc58517024f523 my-vpc	10.0.2.0/24
public-sub-1	subnet-0964ea6f2967de96a	Available	vpc-04acc58517024f523 my-vpc	10.0.1.0/24

(As the requirements of two region in case of load balancer and RDS subnet group so we have to create total 4 subnet (2 private & 2 public) in 2 different region of corresponding subnet)

3. CREATING AN INTERNET GATWAY



4. CREATING NAT GATWAY



5. CREATING TWO ROUTE TABLE

The screenshot shows the 'Create route table' wizard in the AWS VPC console. In the 'Route table settings' step, a new route table named 'route-table' is being created for the VPC 'vpc-04acc58517024f323'. A single tag 'route-table' is added. The 'Create route table' button is at the bottom right.

The screenshot shows the 'Route tables (4)' list in the AWS VPC console. It displays four route tables: 'route-table-public' and 'route-table-private' (both associated with 'vpc-04acc58517024f323') and two unnamed ones (associated with 'vpc-045d0fbca2ea8cbe0' and 'vpc-04acc58517024f523').

6. EDIT SUBNET ASSOCIATIONS

The screenshot shows the 'Edit subnet associations' dialog for route table 'rtb-065c9fdb8f79d2198'. It lists four subnets under 'Available subnets': 'public-sub-2', 'private-sub-1', 'private-sub-2', and 'public-sub-1'. Under 'Selected subnets', 'subnet-05c61d8b6f1f1ea7f / public-sub-2' and 'subnet-0964ea6f2967de96a / public-sub-1' are selected. The 'Save associations' button is at the bottom right.

7. EDIT ROUTE

The screenshot shows two separate instances of the AWS VPC Route Tables 'Edit routes' interface.

Top Window (Route Table ID: rtb-0540c943ae5880b7d):

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-03be53729932ce8cd	-	No

Bottom Window (Route Table ID: rtb-065c9fdb8f79d2198):

Destination	Target	Status	Propagated
10.0.0.16	local	Active	No
0.0.0.0/0	igw-0e0c86f9b9a465374	-	No

In both windows, the 'Save changes' button is highlighted in orange at the bottom right.

The screenshot shows the AWS VPC Management 'Route tables' list interface.

Left Sidebar:

- VPC dashboard
- EC2 Global View
- Filter by VPC: Select a VPC
- Virtual private cloud
 - Your VPCs: New
 - Subnets
 - Route tables
 - Internet gateways
 - Egress-only internet gateways
 - DHCP option sets
 - Elastic IPs
 - Managed prefix lists
 - Endpoints
 - Endpoint services
 - NAT gateways
 - Peering connections
 - Security
 - Network ACLs
 - Security groups
 - DNS firewall
 - Rule groups

Main Content Area:

Route tables (4) Info

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-05ea41e3a391553c2	-	-	Yes	vpc-04acc58517024f323
-	rtb-07f02f6cd6b33fb03	-	-	Yes	vpc-045dfbca2ea8cbe0
route-table-public	rtb-065c9fdb8f79d2198	2 subnets	-	No	vpc-04acc58517024f323
route-table-private	rtb-0540c943ae5880b7d	2 subnets	-	No	vpc-04acc58517024f323

Bottom Panel:

Select a route table

8. CREATE A SECURITY GROUP

The screenshot shows the AWS Cloud Console interface for creating a new security group. The top navigation bar includes links for 'Console Home', 'Route tables | VPC Management', 'Security groups | EC2 | ap-south-1', and a search bar. The main content area is titled 'Create security group' with a sub-link 'Info'. A note states: '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.' The 'Basic details' section contains fields for 'Security group name' (set to 'my-security-gr'), 'Description' (set to 'allow-ssh-http-https'), and 'VPC Info' (set to 'vpc-04acc58517024f323'). The 'Inbound rules' section indicates 'This security group has no inbound rules.' and features a 'Add rule' button. The bottom of the screen shows the AWS navigation bar with links for 'CloudShell', 'Feedback', and various services like CloudWatch Metrics, Lambda, and CloudWatch Logs. The status bar at the bottom right shows network activity, language (ENG IN), and the date/time (12:28 AM 9/21/2023).

This screenshot shows the same 'Create security group' wizard after adding three inbound rules. The 'Inbound rules' section now displays three entries:

Type info	Protocol info	Port range info	Source info	Description - optional info
SSH	TCP	22	Anyw... ▾	<input type="text" value="0.0.0.0/0"/> Delete
HTTP	TCP	80	Anyw... ▾	<input type="text" value="0.0.0.0/0"/> Delete
HTTPS	TCP	443	Anyw... ▾	<input type="text" value="0.0.0.0/0"/> Delete

The rest of the interface remains the same, including the 'Basic details' section and the AWS navigation bar at the bottom.

9. CREATE EC2 INSTANCE IN PUBLIC SUBNET WITH THE CREATED SECURITY GROUP

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The 'Summary' section indicates 1 instance. Under 'Software Image (AMI)', it shows 'Amazon Linux 2 Kernel 5.10 AMI...'. The 'Virtual server type (instance type)' is set to 't2.micro'. The 'Firewall (security group)' is set to 'New security group'. The 'Storage (volumes)' section shows 1 volume(s) - 8 GiB. A tooltip for the 'Free tier' is displayed, stating: '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 GB of snapshots, and 100 GB of bandwidth to the internet.' The 'Launch instance' button is visible at the bottom.

The screenshot shows the 'Network settings' section of the 'Launch an instance' wizard. It specifies a VPC (my-vpc) and a public subnet (public-sub-1). The 'Auto-assign public IP' option is enabled. Under 'Firewall (security groups)', the 'Select existing security group' option is selected, and 'my-security-gr' is chosen. The 'Common security groups' section lists 'my-security-gr sg-047edd22084987caa'. The 'Configure storage' section is partially visible at the bottom. A tooltip for the 'Free tier' is also present on the right side of the screen.

The screenshot shows the AWS EC2 'Launch an instance' wizard. On the left, there are dropdown menus for 'Metadata version', 'Metadata response hop limit', 'Allow tags in metadata', and 'User data - optional'. The 'User data' field contains a base64-encoded shell script to install Apache HTTPD:

```
#!/bin/bash
yum install httpd -y
echo "Hello from - $(hostname)" >/var/www/html/index.html
systemctl start httpd
systemctl enable httpd
```

On the right, the 'Summary' section shows 'Number of instances' set to 1, 'Software Image (AMI)' as Amazon Linux 2023 AMI 2023.1.2..., 'Virtual server type (instance type)' as t2.micro, and 'Firewall (security group)' as my-security-gr. A tooltip for the free tier is displayed, stating: '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 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' At the bottom are 'Cancel', 'Launch instance', and 'Review commands' buttons.

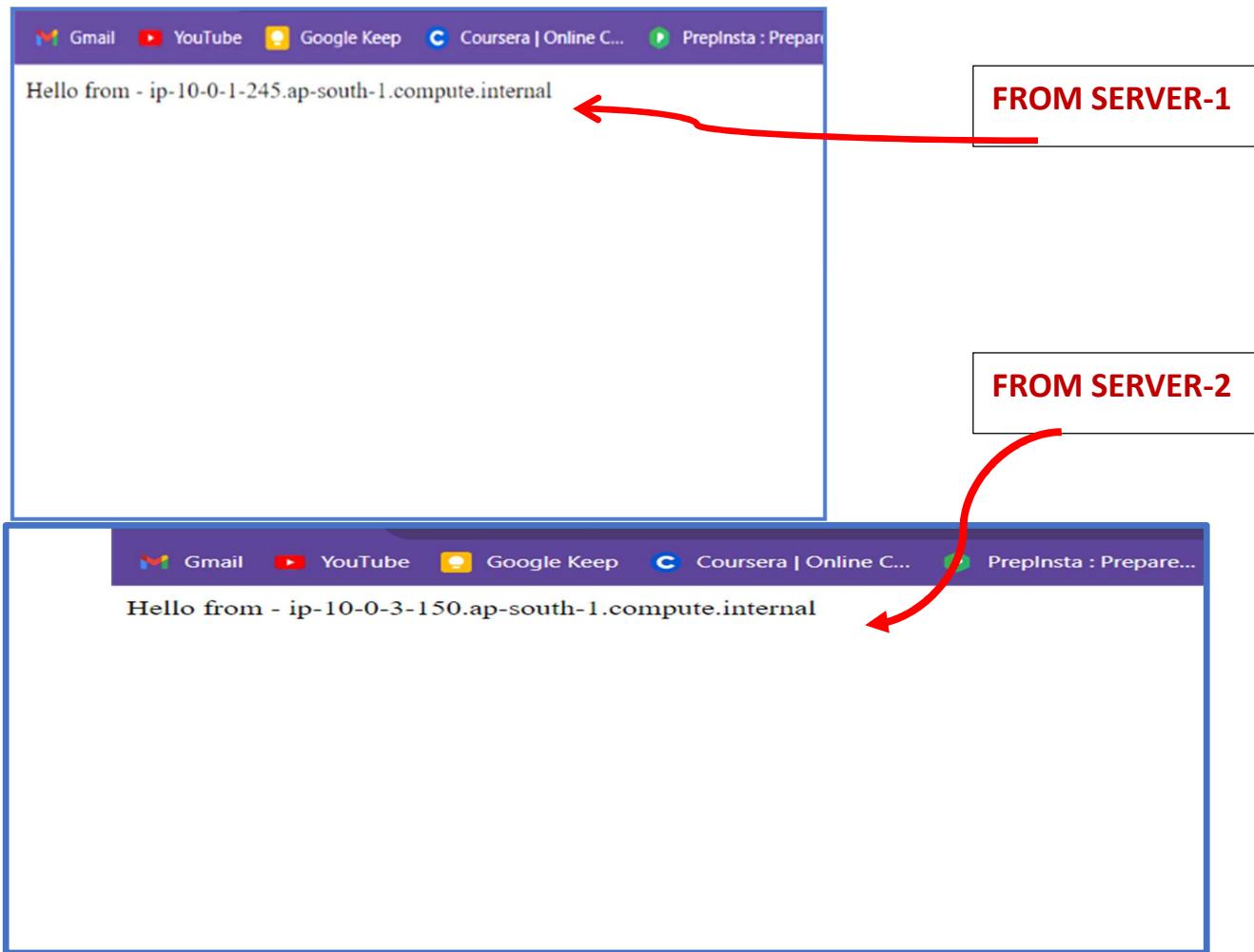
10. SUCCESSFULLY CREATE TWO EC2 INSTANCES AND INSTALL HTTPD WITH HOST NAME

The screenshot shows the AWS EC2 'Instances' page. The sidebar includes links for CloudShell, Feedback, Weather alert (In effect), and various AWS services. The main area displays a table of running instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
WEBSERVER2	i-0c3847ffbae3a3722	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	-
WEB-SERVER	i-0dcc53e5bfc029348	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b	-

A modal window titled 'Select an instance' is open at the bottom.

11. WHEN HIT THE PUBLIC IP



12. CREATE A TARGET GROUP

A screenshot of the AWS Lambda 'Create target group' wizard. The page is titled 'Specify group details' and shows the following steps:

- 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**

The 'Basic configuration' section is expanded, showing the 'Choose a target type' options:

- Instances** (selected):
 - 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: my-target-group

Protocol: HTTP Port: 80
1-65535

VPC: my-vpc
vpc-04acc58517024f523
(IPv4: 10.0.0.0/16)

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.

Health checks

Health check protocol: HTTP

13. REGISTER THE TWO PREVIOUSLY CREATED EC2 INSTANCE AS A TARGET

Step 1: Specify group details

Step 2: Register targets

Available instances (2/2)

Instance ID	Name	State	Security groups	Zone
i-0c3847ffbae3a3722	WEBSERVER2	Running	my-security-gr	ap-south-1a
i-0dcc55e5bf0c029348	WEB-SERVER	Running	my-security-gr	ap-south-1b

2 selected

Ports for the selected instances:
80
1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

Targets (2)

Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet
X	Pending	i-0c3847ffbae3a3722	WEBSERVER2	80	Running	my-security-gr	ap-south-1a	subnet
X	Pending	i-0dcc55e5bf0c029348	WEB-SERVER	80	Running	my-security-gr	ap-south-1b	subnet

2 pending

Create target group

14. CREATE AN APPLICATION LOAD BALANCER

The screenshot shows the AWS CloudShell interface with two tabs open: "Console Home | ap-south-1" and "Create application load balancer". The "Create application load balancer" tab is active, displaying the "Create Application Load Balancer" wizard.

Basic configuration:

- Load balancer name:** load-balancer
- Scheme:** Internet-facing (selected)
- IP address type:** IPv4 (selected)

Mappings:

- ap-south-1a (aps1-az1):** Subnet: subnet-0964ea6f2967de96a, IPv4 address: Assigned by AWS
- ap-south-1b (aps1-az3):** Subnet: subnet-05c61d8b6f1f1ea7f, IPv4 address: Assigned by AWS

Security groups: (Info)

Subnet: subnet-05c61d8b6f1f1ea7f (public-sub-2)

Security groups: my-security-gr

Listeners and routing: Listener HTTP:80

15. ATTACH THE PREVIOUSLY CREATED TARGET GROUP

Protocol: HTTP Port: 80

Default action: Info

Forward to: my-target-group

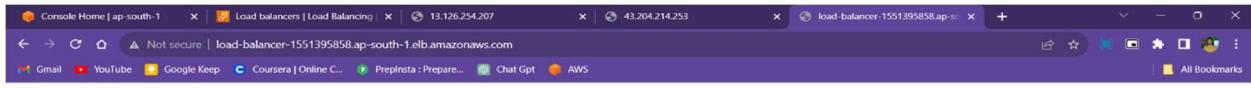
Listener tags - optional:

Add listener tag

Add listener

Add-on services - optional:

16. HIT THE LOAD BALANCER DNS SERVER

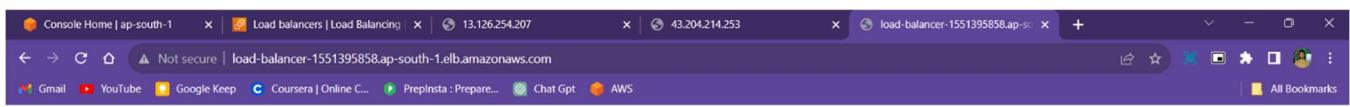


Hello from - ip-10-0-1-245.ap-south-1.compute.internal

This response from server -1

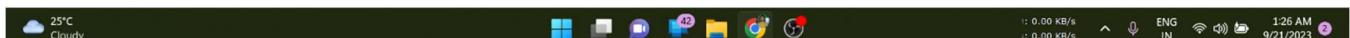


AFTER REFRESH ->



Hello from - ip-10-0-3-150.ap-south-1.compute.internal

This response from server -2



THIS MEANS OUR LOAD BALANCER PERFECTLY WORKING

17.CONFIGURE A SAMPLE WEBSITE IN PREVIOUSLY CREATED EC2 INSTANCE

```
Dashboard | EC2 | ap-south-1 | Connect to instance | EC2 | ap-south-1 | EC2 Instance Connect | ap-south-1 | Sbs Free Website Template | Free | Move File in AWS | + | - | X | 
Gmail YouTube Google Keep Coursera | Online C... Preplinsta : Prepare... Chat Gpt AWS | All Bookmarks | Mumbai | asthalochan | 
aws Services Search [Alt+S] 
inflating: sbs-html/js/revolution/fonts/revicons/revicons90c6.ttf
inflating: sbs-html/js/revolution/fonts/revicons/revicons90c6.woff
creating: sbs-html/js/revolution/
inflating: sbs-html/js/revolution/js/.DS_Store
creating: sbs-html/js/revolution/js/extensions/
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.actions.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.carousel.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.extension肯burn.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.layeranimation.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.migration.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.navigation.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.parallax.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.slideanims.min.js
inflating: sbs-html/js/revolution/js/extensions/revolution.extension.video.min.js
inflating: sbs-html/js/revolution/js/jquery.themepunch.revolution.min.js
inflating: sbs-html/shop.html
inflating: sbs-html/skating.html
[root@ip-10-0-1-175 ~]# ls
sbs.zip
[root@ip-10-0-1-175 ~]# cd sbs-html
[root@ip-10-0-1-175 sbs-html]# ls
about.html contact.html css fonts icon images index.html js shop.html skating.html
[root@ip-10-0-1-175 sbs-html]# cp -r * /var/www/html
[root@ip-10-0-1-175 sbs-html]# cd /var/www/html
[root@ip-10-0-1-175 html]# ls
about.html contact.html css fonts icon images index.html js shop.html skating.html
[root@ip-10-0-1-175 html]# systemctl start httpd
[root@ip-10-0-1-175 html]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-10-0-1-175 html]# 

i-0053b41e10449d684 (web-server)
PublicIPs: 13.126.1.202 PrivateIPs: 10.0.1.175
```

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
26°C Haze 0.19 KB/s ENG IN 4:28 AM 9/21/2023

Dashboard | EC2 | ap-south-1 | Load balancers | Load | EC2 Instance Connect | Sbs Free Website Template | Move File in AWS | sbs | + | - | X |
Gmail YouTube Google Keep Coursera | Online C... Preplinsta : Prepare... Chat Gpt AWS | All Bookmarks | Mumbai | asthalochan |

 [HOME](#) [ABOUT](#) [SKATING](#) [SHOP](#) [CONTACT US](#) [User icon](#) [Search icon](#)

Skating Board School



[READ MORE](#)

26°C Haze 0.00 KB/s 0.00 KB/s ENG IN 4:39 AM 9/21/2023

18. ASSOCIATE AN ELASTIC IP WITH THE EC2 INSTANCE (WEBSERVER)

The screenshot shows the 'Associate Elastic IP address' page in the AWS Management Console. The URL is ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#AssociateAddressPublicIp=52.66.85.255. The page title is 'Associate Elastic IP address'. It asks to choose an instance or network interface to associate with the Elastic IP address (52.66.85.255). The 'Resource type' section has 'Instance' selected. A note states: 'If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account.' Below this, it says: 'If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.' The 'Instance' field contains 'i-0053b41e10449d684'. The 'Private IP address' field is empty. Under 'Reassociation', the checkbox 'Allow this Elastic IP address to be reassociated' is checked. At the bottom are 'Cancel' and 'Associate' buttons.

19. CREATE IMAGE OF THE EC2-INSTANCE(WEBSERVER)

The screenshot shows the 'Create image' page in the AWS Management Console. The URL is ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateImageInstanceId=i-0053b41e10449d684. The page title is 'Create image'. It defines an AMI as a program and settings applied to launch an EC2 instance. The 'Instance ID' is 'i-0053b41e10449d684 (web-server)'. The 'Image name' is 'webserver-img'. The 'Image description - optional' is 'webserver-img'. The 'No reboot' checkbox is unchecked. Under 'Instance volumes', there is one volume listed: 'EBS' (Device: /dev/xvda, Snapshot: Create new snapshot from volume, Size: 8 GiB, Volume type: EBS General Purpose S., IOPS: 100, Throughput: 100 MiB/s, Delete on termination: checked, Encrypted: checked). At the bottom are 'CloudShell' and 'Feedback' buttons, along with system status icons.

20. CREATE A TEMPLATE WITH THE EC2 IMAGE .

The screenshot shows the 'Create launch template' wizard in the AWS Management Console. The 'Summary' section on the right lists the selected software image (webserver-img), virtual server type (t2.micro), and storage (1 volume(s) - 8 GiB). A tooltip for the 'Free tier' indicates it covers 750 hours of t2.micro usage in the first year. The 'Launch template name and description' section contains fields for the name (webserver-tempete) and version (webserver-temp). The 'Auto Scaling guidance' section has a checked checkbox for providing guidance for EC2 Auto Scaling. The 'Launch template contents' section is collapsed. At the bottom, there are 'Cancel' and 'Create launch template' buttons.

The screenshot shows the 'Launch Templates (1/1)' page. It displays a single entry for 'webserver-tempete'. The table columns include Launch Template ID, Launch Template Name, Default Version, Latest Version, Create Time, and Created By. The entry shows 'lt-014b4fd41cb4d0656' as the ID, 'webserver-tempete' as the name, and '1' as both the default and latest version, created on '2023-09-20T23:03:52.000Z' by 'arn:aws:iam::179916895369:root'. Below the table, the 'Launch template details' section shows the same information. The 'Launch template version details' section shows a single version entry with the same details. Navigation buttons like 'Actions', 'Delete template', and 'Create launch template' are visible at the top and bottom of the pages.

21. SETUP AUTO SCALING GROUP

The screenshots illustrate the step-by-step configuration of an Auto Scaling Group in the AWS Management Console.

Screenshot 1: Choose launch template or configuration

This step involves naming the Auto Scaling group and selecting a launch template. The 'Name' field contains 'Scaling-group'. The 'Launch template' dropdown shows 'webserver-temp-templete' (Default 1). The 'Description' field is 'webserver-temp' and the 'Instance type' is 't3.micro'.

Screenshot 2: Choose instance launch options

This step focuses on VPC settings. The 'Network' section shows the selected VPC as 'vpc-04acc58517024f523 (my-vpc)'. Under 'Availability Zones and subnets', two subnets are listed: 'ap-south-1b | subnet-05c61d8b6f1f1ea7f (public-sub-2)' and 'ap-south-1a | subnet-0964ea6f2967de96a (public-sub-1)'. A 'Create a subnet' button is also present.

Screenshot 3: Attach to an existing load balancer

This step allows attaching the Auto Scaling group to an existing load balancer. It shows three options: 'No load balancer' (selected), 'Attach to an existing load balancer' (selected), and 'Attach to a new load balancer'. The 'Attach to an existing load balancer' section includes a 'Choose from your load balancer target groups' button and a dropdown menu showing 'my-target-gr | HTTP Application Load Balancer: my-load-balancer'.

The screenshot shows the AWS EC2 Auto Scaling groups page. The top navigation bar includes links for Dashboard, Auto Scaling groups, EC2 Instance Connect, Sbs Free Website Template, Move File in AWS, and sbs. The AWS logo and search bar are also present. The main content area displays one Auto Scaling group named "Scaling-group" with the following details:

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability zone
Scaling-group	webserver-template Version Default	1	-	1	1	3	ap-south-1...

At the bottom, it says "0 Auto Scaling groups selected". The status bar at the bottom right shows system information like temperature (26°C), battery level (Haze), network speed (4.08 KB/s, 0.82 KB/s), and date/time (4:42 AM, 9/21/2023).

22. CREATE TWO CLOUD WATCH ALARMS USING CPU UTILIZATION METRIC

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

Percent

24

12.1

0.235

20:30 21:30 22:30

CPUUtilization

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-0053b41e10449d684

Instance name
web-server

Statistic
Average

Period
1 minute

CloudWatch

Favorites and recent

Alarms ▲ 0 ○ 0 ○ 0

In alarm

All alarms

Logs

Metrics

X-Ray traces

Events

Application monitoring

Insights

Settings

Getting Started

What's new [New](#)

CloudWatch > Alarms

Successfully created alarm scale-out.

CloudWatch > Alarms

Alarms (2)

Hide Auto Scaling alarms

Create composite alarm

Actions

Create alarm

Name	State	Last state update	Conditions	Actions
scale-out	Insufficient data	2023-09-20 23:15:48	CPUUtilization <= 40 for 1 datapoints within 1 minute	No actions
scale-in	Insufficient data	2023-09-20 23:14:51	CPUUtilization >= 60 for 1 datapoints within 1 minute	No actions

23. ATTACH TWO DYNAMIC POLICY IN AUTO SCALING GROUP (SCALE IN & SCALE OUT)

The screenshot shows the AWS CloudWatch Metrics Insights interface. At the top, there are two tabs: "Metrics" and "Logs". Below them, a search bar contains the query "awslogs -filter @version=1 @timestamp >= 2023-09-21T00:00:00 & @timestamp <= 2023-09-21T12:00:00". The main area displays two insights results:

- CloudWatch Metrics Insights 1**: This insight shows a single metric named "CPUUtilization" with a value of 60. It includes a detailed breakdown of the metric data over time.
- CloudWatch Metrics Insights 2**: This insight shows a single metric named "CPUUtilization" with a value of 60. It includes a detailed breakdown of the metric data over time.

The screenshot shows the AWS CloudWatch Metrics Insights interface. At the top, there are two tabs: "Metrics" and "Logs". Below them, a search bar contains the query "awslogs -filter @version=1 @timestamp >= 2023-09-21T00:00:00 & @timestamp <= 2023-09-21T12:00:00". The main area displays two insights results:

- CloudWatch Metrics Insights 1**: This insight shows a single metric named "CPUUtilization" with a value of 60. It includes a detailed breakdown of the metric data over time.
- CloudWatch Metrics Insights 2**: This insight shows a single metric named "CPUUtilization" with a value of 60. It includes a detailed breakdown of the metric data over time.

The screenshot shows the AWS CloudShell interface with the following details:

- Policy type:** Simple scaling
- Scaling policy name:** scale-out
- CloudWatch alarm:** scale-out (Choose an alarm that can scale capacity whenever: scale-out). A note indicates: "breaches the alarm threshold: CPUUtilization <= 40 for 1 consecutive periods of 60 seconds for the metric dimensions: InstanceId = i-04e8432290187f044".
- Take the action:** Remove 1 capacity units.
- And then wait:** 3d seconds before allowing another scaling activity.

At the bottom right of the CloudShell window, there are status icons for network speed (0.82 KB/s, 0.59 KB/s), language (ENG IN), and time (4:46 AM, 9/21/2023).

24. INCREASE THE CPU UTILIZATION FOR CHECKING AUTO SCALING

The screenshot shows the AWS CloudShell interface with the following terminal output:

```
Last login: Wed Sep 20 22:50:12 2023
[root@ip-10-0-3-62 ~]# Amazon Linux 2 AMI
[root@ip-10-0-3-62 ~]#
https://aws.amazon.com/amazon-linux-2/
5 package(s) needed for security, out of 9 available
Run "sudo yum update" to apply all updates.
[root@ip-10-0-3-62 ~]# sudo su
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[1] 2973
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[2] 2974
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[3] 2975
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[4] 2976
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[5] 2977
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[6] 2978
[root@ip-10-0-3-62 ~]# yes> /dev/null &
[7] 2979
[root@ip-10-0-3-62 ~]#
```

i-0a70ed52a0d664705

PublicIPs: 65.0.97.31 PrivateIPs: 10.0.3.62



ONE EC2-INSTANCE AUTOMATICALLY CREATED AND RUN

(IT MEANS OUR AUTO SCALING GROUP WORKING PERFECTLY)

A screenshot of the AWS EC2 Instances page. The left sidebar shows 'Instances' selected. The main area displays a table of instances with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP. Three instances are listed:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
web-server	i-0053b41e10449d684	Running	t2.micro	2/2 checks passed	1/1 has no data	ap-south-1a	-
-	i-0a70ed52a0d664705	Running	t3.micro	2/2 checks passed	No alarms	ap-south-1b	-
-	i-0513b1f96733380fa	Running	t3.micro	Initializing	No alarms	ap-south-1a	-

25. CREATE A SUBNET GROUP IN AMAZON RDS DASHBOARD

A screenshot of the AWS RDS Subnet Groups page. The left sidebar shows 'Subnet groups' selected. The main area shows the creation of a new subnet group:

- Subnet group details:**
 - Name: db-sb-group
 - Description: db-sunet
 - VPC: my-vpc (vpc-04acc58517024f323)
- Add subnets:**
 - Availability Zones:** Choose the Availability Zones that include the subnets you want to add. (Choose an availability zone dropdown)
 - Subnets:** Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones. (Select subnets dropdown)
 - Subnets selected: ap-south-1a, ap-south-1b

HERE I SELECT
PRIVATE SUBNET

26. CREATE A RDS DATABASE

The screenshot shows the 'Create database' wizard for MySQL. On the left, under 'Choose a database creation method', 'Standard create' is selected. In the 'Engine options' section, 'MySQL' is chosen from a list that includes Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), MariaDB, PostgreSQL, and Oracle. To the right, a detailed description of MySQL is provided, highlighting its popularity and various features like support for up to 64 TiB, General Purpose, Memory Optimized, and Burstable Performance instance classes, automated backup, point-in-time recovery, and up to 15 Read Replicas.

This screenshot shows the 'Availability and durability' configuration step. It offers three deployment options: Multi-AZ DB Cluster (new), Multi-AZ DB instance, and Single DB instance. 'Single DB instance' is selected. The 'Settings' section allows setting the database identifier to 'database-1'. Under 'Credentials Settings', the master username is set to 'admin'. A note about managing master credentials in AWS Secrets Manager is present. The right panel continues the MySQL description.

The screenshot shows the 'Public access' configuration step. It provides two options: 'Yes' (allowing public IP access) and 'No' (restricting access to the VPC). 'No' is selected. Below this, the 'VPC security group (firewall)' section allows choosing or creating a new VPC security group, with 'my-security-gr' selected. The 'Existing VPC security groups' dropdown also lists 'my-security-gr'. The 'Availability Zone' dropdown shows 'No preference'. At the bottom, there's a note about RDS Proxy and a checkbox for creating it.

Amazon RDS

database-1

Summary

DB identifier	CPU	Status	Class
database-1	2.92%	Backing-up	db.m6gd.large
Role	Current activity	Engine	Region & AZ
Instance	0.00 sessions	MySQL Community	ap-south-1b

Connectivity & security

Endpoint & port	Networking	Security
Endpoint database-1.cy2hingkatkm.ap-south-1.rds.amazonaws.com	Availability Zone ap-south-1b	VPC security groups my-security-gr (sg-047edd22084987caa) Active
Port 3306	VPC my-vpc (vpc-04acc58517024f323)	Publicly accessible No
	Subnet group db-sb-group	Certificate authority Info rds-ca-2019
	Subnets subnet-0531cd1551d9a1x0a	

CloudShell Feedback 26°C Haze © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 5:35 AM 9/21/2023

27. TO CONNECT OUR DATABASE WITH OUR LOCAL SYSTEM I HAVE TO LAUNCH A VPN EC2-INSTANCE WITH OUR PUBLIC SUBNET

Launch an instance | Databases | RDS | ap- | Auto Scaling group | Alarms | CloudWatch | Generate CPU and Mem | create cpu load in p | New Tab

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

Gmail YouTube Google Keep Coursera Online C... Preplinsta : Prepare... Chat Gpt AWS

Services Search [Alt+S]

CloudShell Feedback 26°C Haze © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences ENG IN 5:30 AM 9/21/2023

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Selected AMI: (ami-067c21fb1979f0b27) (Quickstart AMIs)

open vpn

Quickstart AMIs (0) My AMIs (0) AWS Marketplace AMIs (63) Community AMIs (33)

Refine results Clear all filters Operating system Linux/Unix All Linux/Unix Amazon Linux CentOS Debian Fedora Gentoo

open vpn (33 filtered, 33 unfiltered)

Community AMIs

Community AMIs contain all AMIs that are public, therefore anyone can publish an AMI and it will show in this catalog. This catalog can also contain paid products. When using community AMIs it is best practice to ensure you know and trust the publisher before launching an AMI.

OpenVPN Access Server QA Image-bbfff26cd-b407-44a2-a7ef-70b8971391f1

Select

ami-02baa177a7bc0e192 OpenVPN Access Server 2.11.3 publisher image from https://www.openvpn.net/. OwnerAlias: aws-marketplace Platform: Other Linux Architecture: x86_64 Owner: G79593335241 Publish date: 2023-03-08 Root device type: ebs Virtualization: hvm ENA enabled: Yes

The screenshot shows the AWS EC2 console with the 'Launch Instances' wizard open. The left sidebar lists services like Databases, Auto Scaling group, Alarms, Generate CPU and Mem, and New Tab. The main area is titled 'Launch instances' and shows the following steps:

- Step 1: Set instance details**
 - Instance type:** t2.micro (Free tier)
 - Number of instances:** 1
 - Software image (AMI):** OpenVPN Access Server QA Image... (ami-02baa177a7bc0e192)
 - Virtual server type (instance type):** m4.large
 - Firewall (security group):** New security group
 - Storage (volumes):** 1 volume(s) - 8 GiB
- Step 2: Configure network**
 - Network settings:** Info
 - VPC - required:** vpc-04acc58517024f325 (my-vpc) 10.0.0.0/16
 - Subnet:** subnet-05c61d8b6f1f1ea7f (public-sub-2)
 - VPC: vpc-04acc58517024f325 Owner: 179916895369 Availability Zone: ap-south-1b IP addresses available: 249 CIDR: 10.0.3.0/24
 - Auto-assign public IP:** Info
 - Firewall (security groups):** Info
 - Create security group
 - Select existing security group
 - Security group name - required:** OpenVPN Access Server (50 Connected Devices)-2.11.3-AutogenByAWSMP--2
 - Description - required:** OpenVPN Access Server (50 Connected Devices)-2.11.3-AutogenByAWSMP--2 creat
 - Inbound Security Group Rules:** (Empty)
- Step 3: Review and launch**
 - Review commands:** (button)
 - Launch instance:** (button)
 - Cancel:** (button)

28. CONNECT THE VPN SERVER EC2-INSTANCE AND SETUP IT

```
Connect to instance x EC2 Instance Con x RDS | ap-south-1 x Auto Scaling gro x Alarms | CloudW x Generate CPU an x create cpu load i x OpenVPN Login x + 
ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connType=standard&instanceId=i-0eaea6f932f794d7c&osUser=root&sshPort=22#/ 
Gmail YouTube Google Keep Coursera | Online C... Preplinsta : Prepare... Chat Gpt AWS 
Services Search [Alt+S] Mumbai asthalochan

Adding web group account...
Adding web group...
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.11.3...
Generating PAM config for openvpnas ...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service → /lib/systemd/system/openvpnas.service.
Starting openvpnas...

NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly. Please ensure that your time and date
are correct on this system.

Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:

https://13.127.245.255:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin UI: https://13.127.245.255:943/admin
Client UI: https://13.127.245.255:943/
To login please use the "openvpn" account with "ZEJvNWDEXpmY" password.

See the Release Notes for this release at:
https://openvpn.net/vpn-server-resources/release-notes/

root@ip-10-0-3-52:~# ^C
root@ip-10-0-3-52:~# 

i-0eaea6f932f794d7c (openvpn)
PublicIPs: 13.127.245.255 PrivateIPs: 10.0.3.52

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
26°C Haze 42 5:36 AM
:: 2.73 KB/s :: 0.71 KB/s ENG IN 9/21/2023
```

Status Overview

VPN services are currently ON

Active Configuration

Access Server version:	2.11.3
Server Name:	43.204.130.129
Allowed VPN Connections:	50 VPN Connections
Current Active Users:	0
Authenticate users with:	local
Accepting VPN client connections on IP address:	all interfaces
Port for VPN client connections:	tcp/443, udp/1194
OSI Layer:	3 (routing/NAT)
Clients access private subnets using:	NAT

POWERED BY OPENVPN
© 2009-2023 OpenVPN Inc.
All Rights Reserved

26°C Haze

Active Configuration

Import Profile

Access Server version:	2.11.3
Server Name:	43.204.130.129
Allowed VPN Connections:	50 VPN Connections
Current Active Users:	0
Authenticate users with:	local
Accepting VPN client connections on IP address:	all interfaces
Port for VPN client connections:	tcp/443, udp/1194
OSI Layer:	3 (routing/NAT)
Clients access private subnets using:	NAT

POWERED BY OPENVPN
© 2009-2023 OpenVPN Inc.
All Rights Reserved

26°C Haze

OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile
openvpn@43.204.130.129

DISCONNECTED

CONNECTION STATS

3.7KB/s

0B/s

BYTES IN 670 B/S BYTES OUT 312 B/S

DURATION 00:00:07

PACKET RECEIVED 3 sec ago

aws Services Search

Adding web group account...
Adding web group...
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.11.3...
Generating PAM config for openvpnas...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service.
Starting openvpnas...

NOTE: Your system clock must be correct for OpenVPN Access Server to perform correctly. Please ensure that your time and date are correct on this system.

Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by directing your Web browser to this URL:
<https://43.204.130.129:943/admin>

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin UI: <https://43.204.130.129:943/admin>
Client UI: <https://43.204.130.129:943/>
To login please use the "openvpn" account with "1YQe1IdDNKp" password.

See the Release Notes for this release at:
<https://openvpn.net/vpn-server-resources/release-notes/>

```
root@ip-10-0-3-64:~# ^C
root@ip-10-0-3-64:~# ]
```

i-0347a5b869299f564 (openvpn)
PublicIPs: 43.204.130.129 PrivateIPs: 10.0.3.64

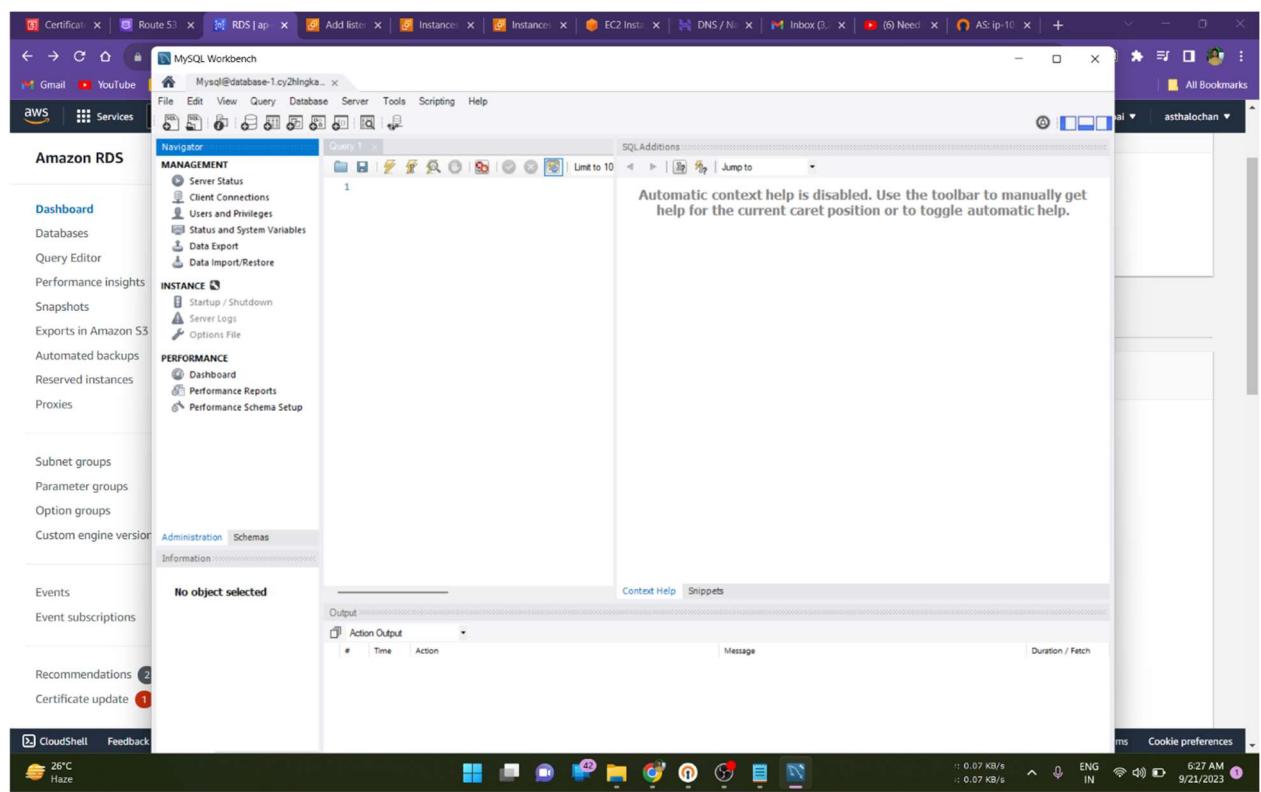
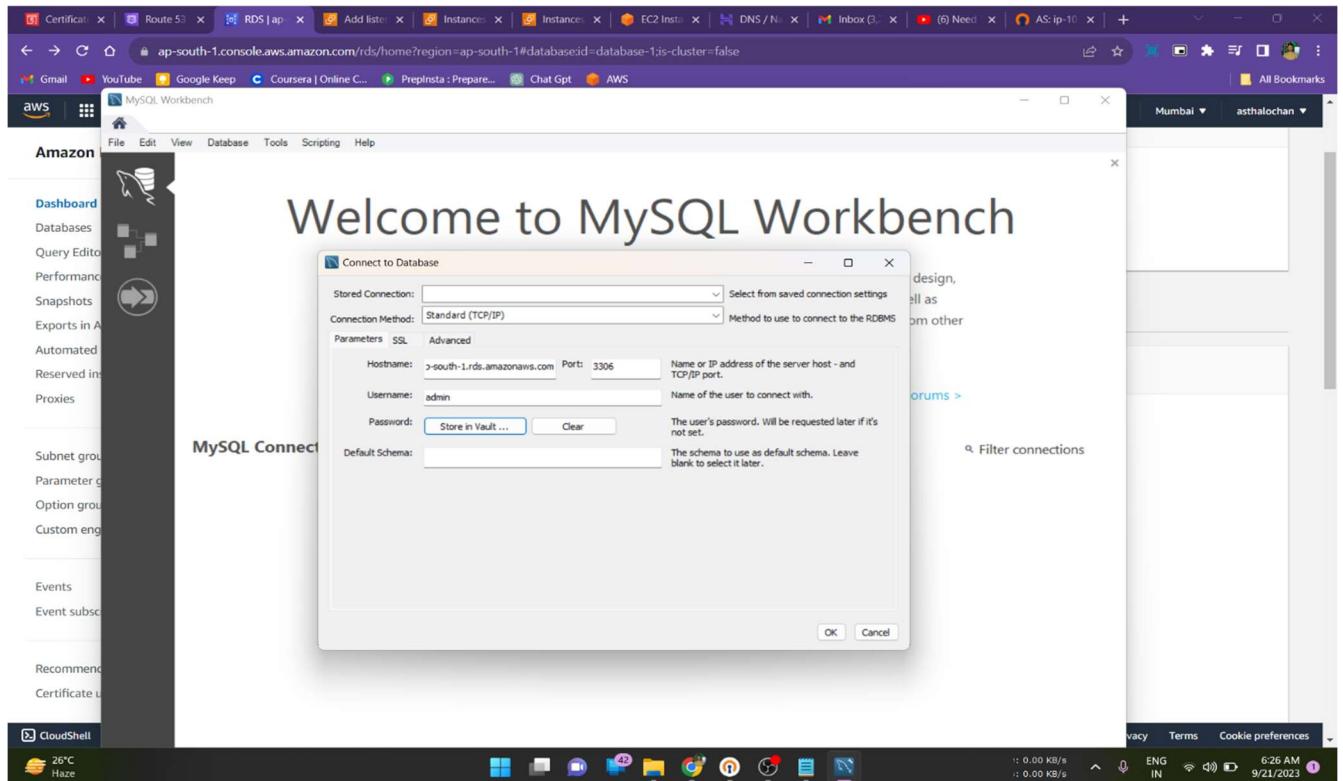
CloudShell Feedback

26°C Haze

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

11.8 KB/s ENG IN 625 AM 9/21/2023

**29. AFTER CONNECTING VPN,
OPEN MYSQL WORK BENCH IN
LOCAL SYSTEM AND CONNECT IT WITH THE HELP OF
RDS DATABASE ENDPOINT PORT AND LOGIN CREDENTIADS**



RDS MYSQL DATABASE SUCESSFULLY CONNECTED

30. REQUEST A PUBLIC CERTIFICATE WITH OWN DOMAIN NAME

AWS Certificate Manager > Certificates > Request certificate > Request public certificate

Domain names
Provide one or more domain names for your certificate.

Fully qualified domain name [Info](#)
asthalochan.tech [Remove](#)

*.asthalochan.tech [Remove](#)

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.

AWS Certificate Manager > Certificates > 6fc1e4fd-24d5-46b0-acea-e4e32129c56b

Certificate status

Identifier
6fc1e4fd-24d5-46b0-acea-e4e32129c56b

ARN
arn:aws:acm:ap-south-1:179916895369:certificate/6fc1e4fd-24d5-46b0-acea-e4e32129c56b

Type
Amazon Issued

Status [Pending validation](#) [Info](#)

Domains (2)

Domain	Status	Renewal status	Type	CNAME name	CNAME value
asthalochan.tech	Pending validation	-			
*.asthalochan.tech	Pending validation	-			

[Create records in Route 53](#) [Export to CSV](#)

Details

CloudShell Feedback 30°C Mostly cloudy 2:55 PM 9/21/2023

VALIDATION PENDING

31. CREATE A HOSTED ZONE IN AWS ROUTE 53

The screenshot shows the 'Create record' interface in the AWS Route 53 service. The 'Record name' field contains 'subdomain' and the 'Record type' field is set to 'A'. The 'Route traffic to' section is configured with an Application Load Balancer named 'dualstack.my-load-balancer-51969533.ap-south-1.elb.amazonaws.com'. The 'Routing policy' is set to 'Simple routing' and 'Evaluate target health' is enabled. The status bar at the bottom indicates network speed (5.85 KB/s), language (ENG IN), and date (9/21/2023).

32. CREATE RECORD WITH LOAD BALANCER

This screenshot is identical to the one above, showing the 'Create record' interface in the AWS Route 53 service. It displays the same configuration for an A record named 'subdomain' pointing to an Application Load Balancer. The status bar at the bottom is identical, showing network speed (5.85 KB/s), language (ENG IN), and date (9/21/2023).

Screenshot of the AWS Route 53 console showing the 'asthalochan.tech' hosted zone details. The left sidebar lists various Route 53 features like Hosted zones, IP-based routing, Traffic flow, Domains, and Resolver. The main pane displays the 'Hosted zone details' for 'asthalochan.tech' with three records listed:

Type	Value/Route traffic to	TTL (s...)	Health ...
NS	ns-1611.awsdns-09.co.uk. ns-1501.awsdns-59.org. ns-858.awsdns-43.net. ns-315.awsdns-39.com.	172800	-
SOA	ns-1611.awsdns-09.co.uk. a...	900	-
A	dualstack.my-load-balancer....	-	-

33.as our ssl certificate not issued so it's showing insecure

Screenshot of a web browser showing a warning message: 'Not secure | aws.asthalochan.tech'. The URL 'aws.asthalochan.tech' is highlighted with a red arrow. The page content is for 'Skating Board School' (SBS) featuring two cartoon skaters on a purple wave.

Skating Board School

HOME ABOUT SKATING SHOP CONTACT US

READ MORE

88°F Rain coming

34. ADD LISTENER IN LOAD BALANCER

The screenshot shows the AWS CloudFront console with the URL ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ElbAddListener:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:179916895369:loadbalancer/ap.... The page title is "Add listener | Load Balancer". The main content area is titled "Add listener" and "Info". It describes adding a listener to an Application Load Balancer (ALB) to define how client requests and network traffic are routed within your application. A section titled "Load balancer details: my-load-balancer" is shown. Under "Listener details: HTTP:82", it says "Protocol : Port" and "The listener will be identified by the protocol and port." A dropdown menu shows "HTTP" selected with "82" in the input field. Below this, there's a note about redirecting client requests from one URL to another, mentioning HTTPS to HTTP. Under "Default actions" (Info), it says "The default action is used if no other rules apply. Choose the default action for traffic on this listener." There are three radio button options: "Forward to target groups" (unchecked), "Redirect to URL" (checked), and "Return fixed response" (unchecked). The "Redirect to URL" section is expanded, showing "URI parts" and "Full URL" tabs. The "Full URL" tab is selected, showing the URL "https://asthalochan.tech". At the bottom, there are "Cancel" and "Add" buttons.

This screenshot is identical to the one above, showing the "Add listener" step for an Application Load Balancer. The URL and page title remain the same. The main content area is titled "Add listener" and "Info". It describes adding a listener to an Application Load Balancer (ALB) to define how client requests and network traffic are routed within your application. A section titled "Load balancer details: my-load-balancer" is shown. Under "Listener details: HTTP:82", it says "Protocol : Port" and "The listener will be identified by the protocol and port." A dropdown menu shows "HTTP" selected with "82" in the input field. Below this, there's a note about redirecting client requests from one URL to another, mentioning HTTPS to HTTP. Under "Default actions" (Info), it says "The default action is used if no other rules apply. Choose the default action for traffic on this listener." There are three radio button options: "Forward to target groups" (unchecked), "Redirect to URL" (checked), and "Return fixed response" (unchecked). The "Redirect to URL" section is expanded, showing "URI parts" and "Full URL" tabs. The "Full URL" tab is selected, showing the URL "https://asthalochan.tech". At the bottom, there are "Cancel" and "Add" buttons.