ALB Log Analytics and Monitoring using AWS S3, Athena, and QuickSight

Refer these links for more info or query
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/enable-access-logging.html > for bucket policy

https://docs.aws.amazon.com/athena/latest/ug/create-alb-access-logs-table.html >for athena query

Step 1: Create a Launch Template

A launch template defines the AMI, instance type, security group, and other settings for your EC2 instances.

1. **Go to AWS Console → EC2**
2. Click **Launch Templates → Create Launch Template**
3. **Enter a Name** (e.g., `my-launch-template`)
4. **Choose AMI** (Amazon Linux.)
5. **Choose Instance Type** (e.g., `t2.micro`)
6. **Select Key Pair** (for SSH access)
7. **Select Security Group** (Allow HTTP, HTTPS, and SSH)
8. **Configure Storage** (Default is 8GB for Amazon Linux 2)

Add User Data for automatic bootstrapping (e.g., installing a web server)

#!/bin/bash

sudo yum update

sudo yum install httpd -y

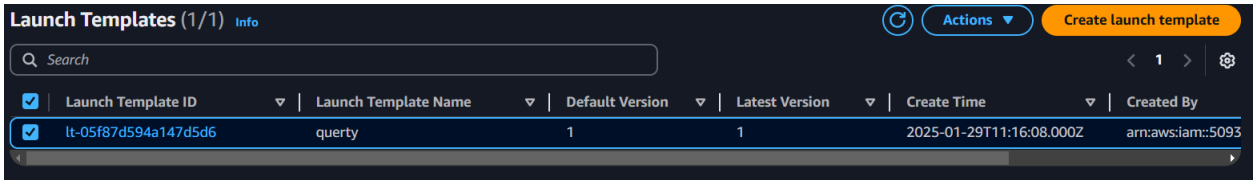
sudo systemctl start httpd

sudo systemctl enable httpd

sudo wget https://www.free-css.com/assets/files/free-css-templates/download/page296/finexo.zip

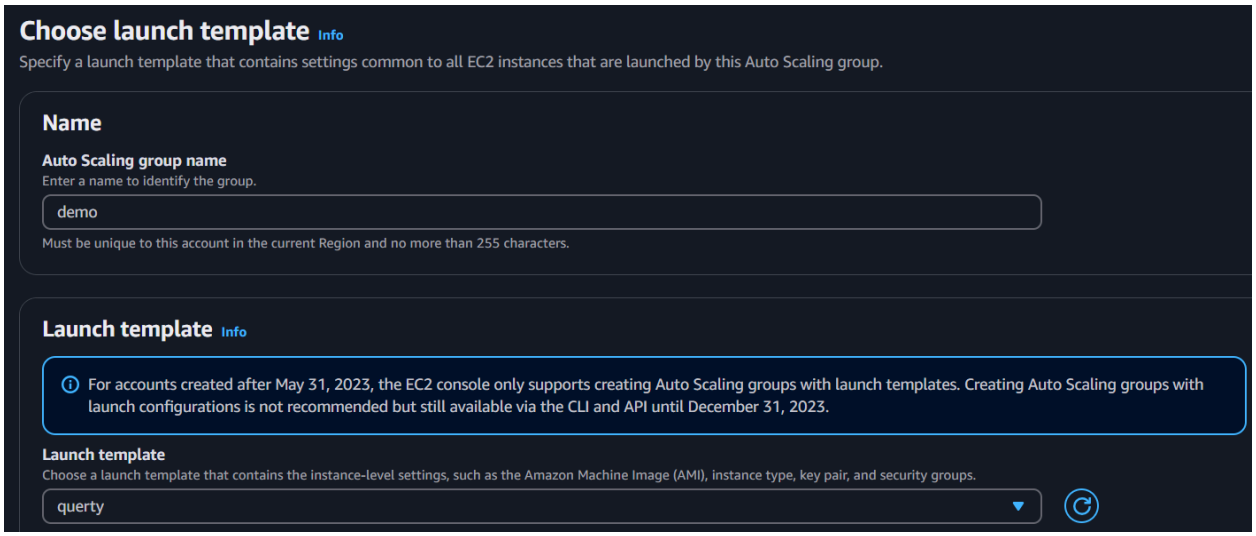
sudo unzip finexo.zip

sudo mv finexo-html/* /var/www/html/



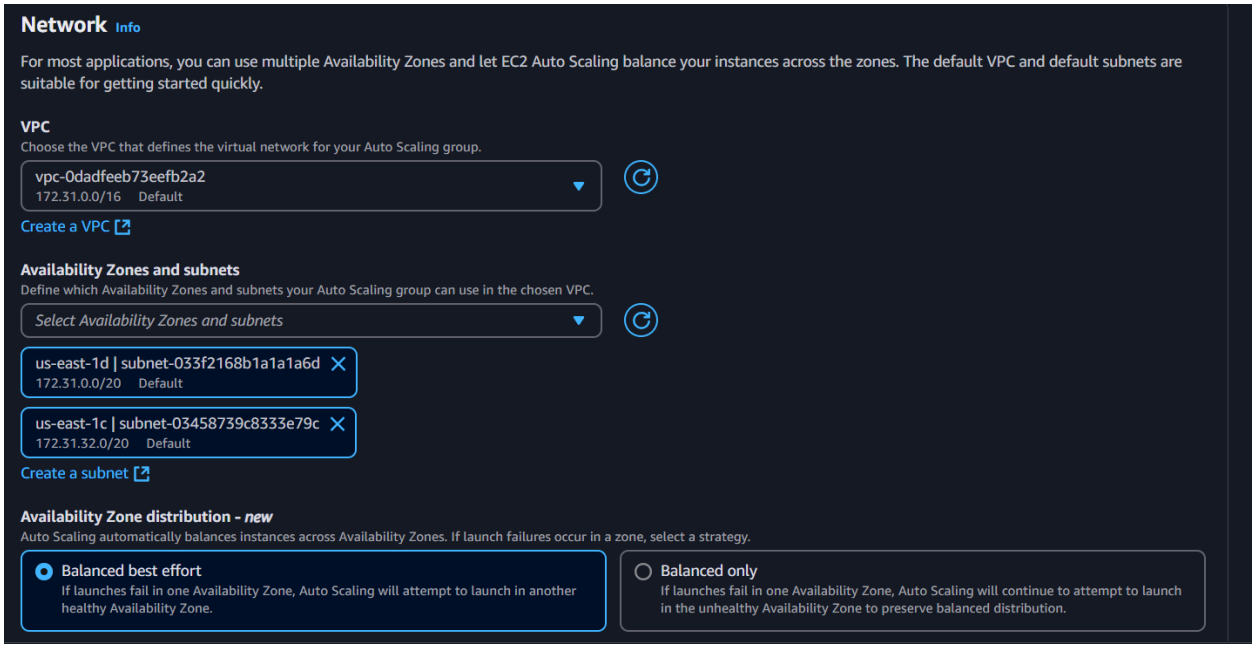
Step 2: Create an Auto Scaling Group (ASG)

1. Go to **EC2 Dashboard → Auto Scaling Groups**
2. Click **Create Auto Scaling Group**
3. **Enter Name** (e.g., `my-asg`)
4. **Choose Launch Template** (Select the template created in Step 1)
5. Click **Next**



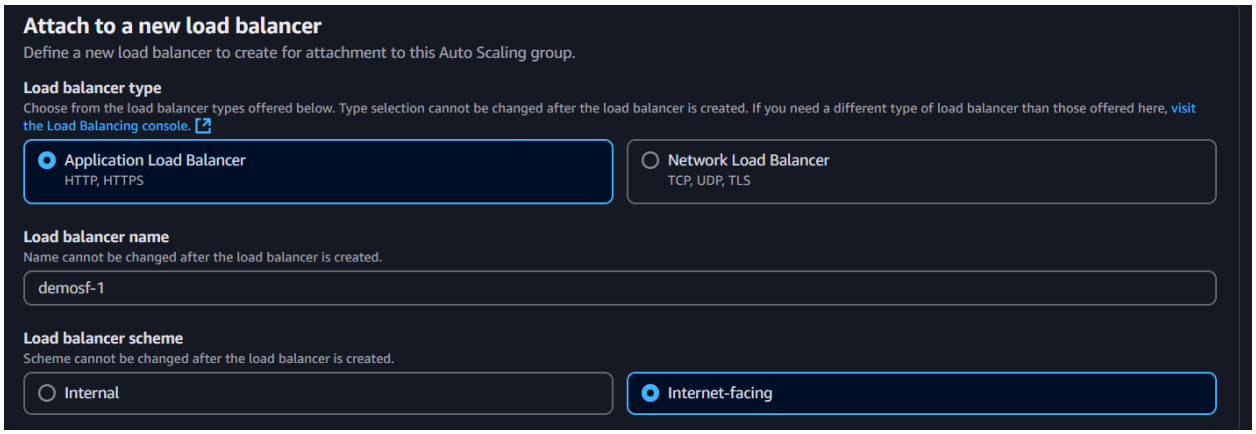
Configure Network

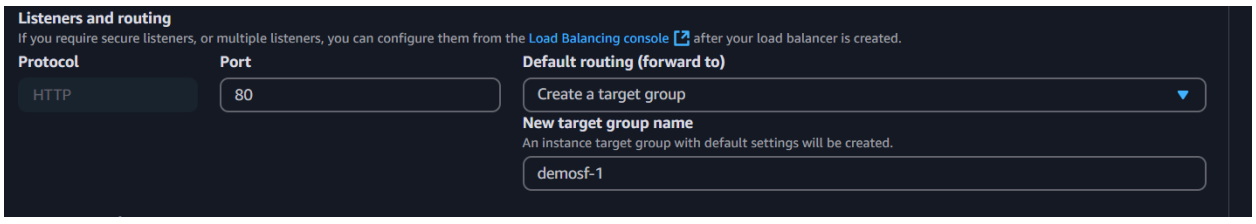
6. Select **VPC** (Default or Custom)
7. Select **Subnets** (Choose at least 2 different AZs for HA)
8. Click **Next**



Configure Load balancing

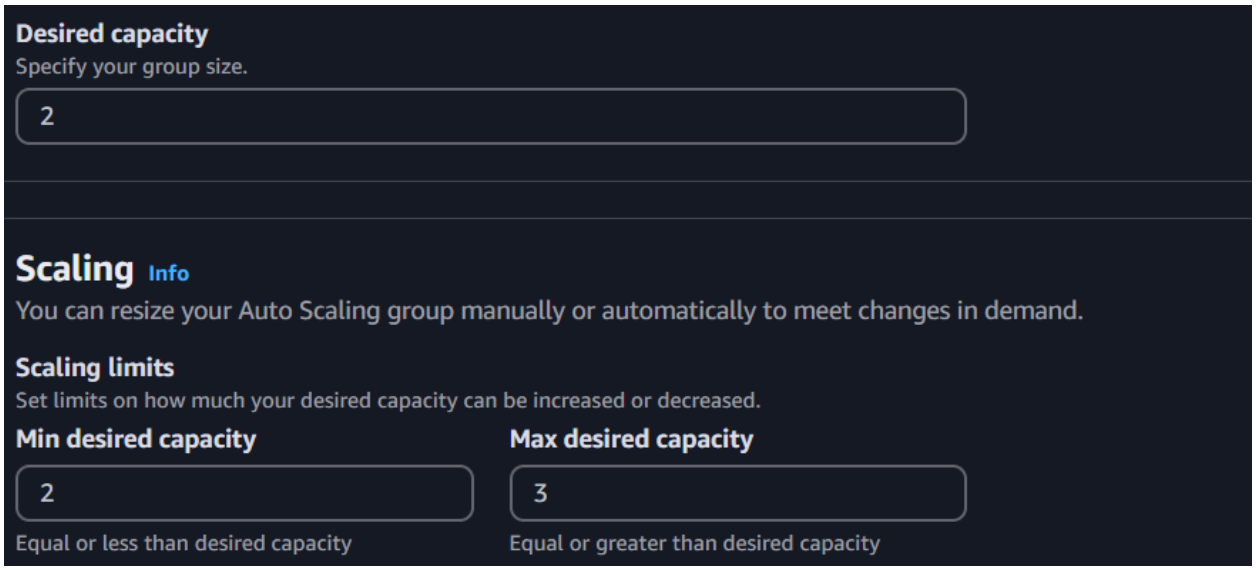
1. Attach new load balancer
2. Application Load Balancer
3. Enter Name: `my-alb`
4. Scheme: Internet-facing
5. Create a Target Group:
6. **Name: `my-target-group`**

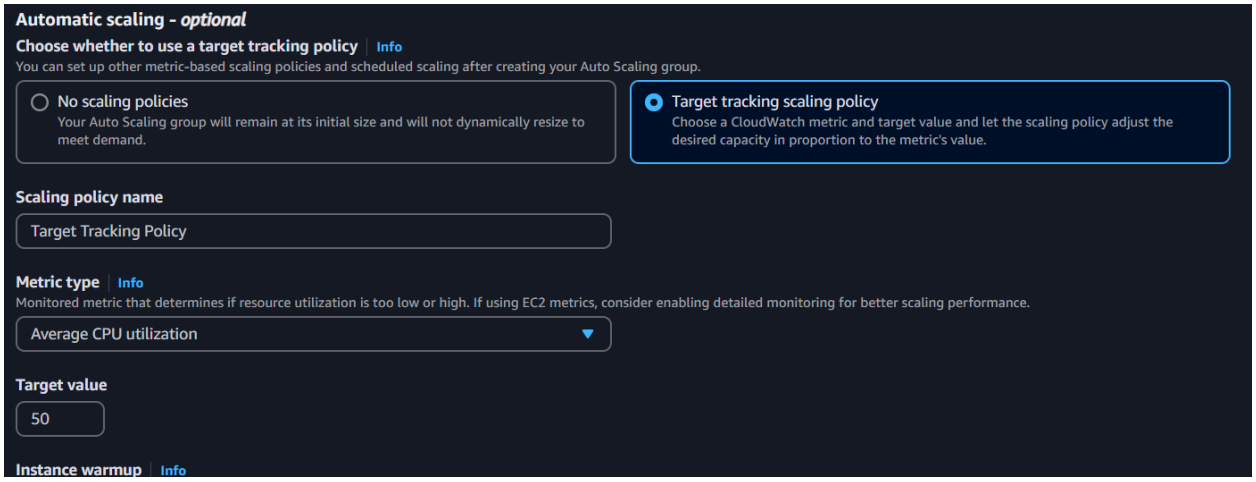




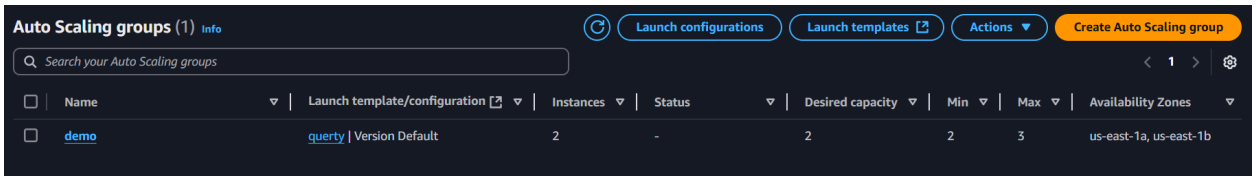
Configure Scaling Policy

9. Choose **Desired Capacity** (e.g., 2)
10. Set **Minimum Instances** (2)
11. Set **Maximum Instances** (3)
12. Enable **Scaling Policies** (optional, to scale based on CPU usage)



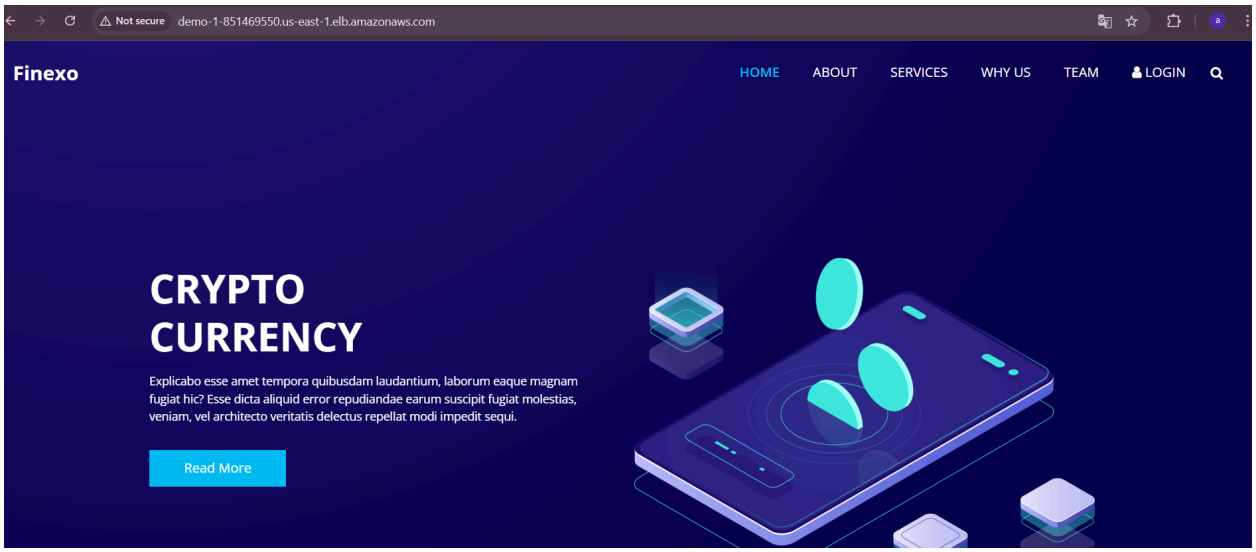


Auto scaling group is created



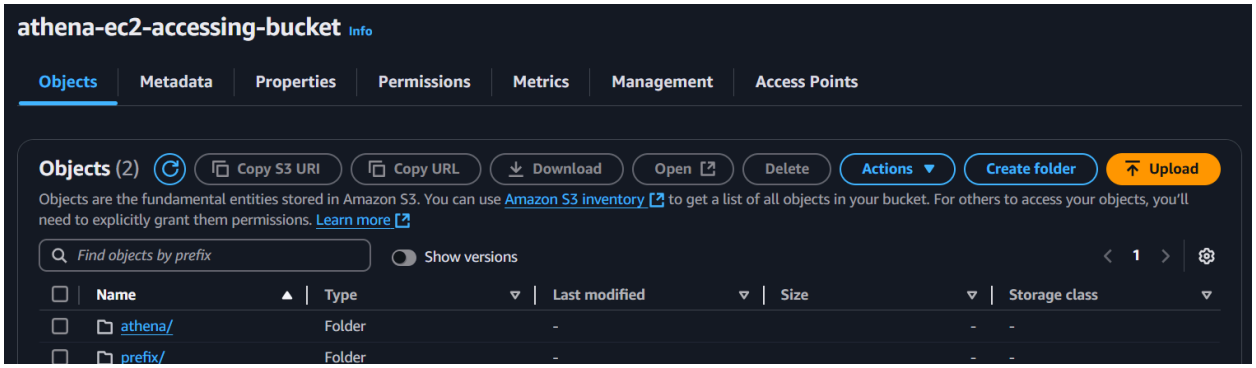
Step 3: Test the Setup

1. Go to **EC2** → **Load Balancers** → Copy the **ALB DNS Name**
2. Open the DNS in a browser → You should see **your webpage**



Step 4: Create an S3 Bucket with a Prefix (Folder)

1. **Go to S3 Console:**
   - Navigate to the **AWS S3 service**
   - Click **Create Bucket**
2. **Enter Bucket Name:**
   - Choose a **globally unique name** (e.g., `my-alb-logs-bucket`)
   - Select your **AWS region** (e.g., `us-east-1`)
3. **Configure Settings:**
   - **Disable Block Public Access (optional, but recommended)**
   - **Enable Object Ownership** (ACLs enabled)
4. **Click Create Bucket**
5. **Create a Prefix (Folder):**
   - Click on your newly created bucket
   - Click **Create Folder**
   - Enter a **prefix name** (e.g., `alb-logs/`)
   - Click **Create Folder**



Step 5: Set S3 Bucket Policy for ALB Logs in `us-east-1` Region

1. Go to the AWS Console → S3 Service
2. Select Your Bucket (`my-alb-logs-bucket`)
3. Click Permissions → Bucket Policy
4. Paste the following JSON policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::127311923021:root"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::athena-ec2-accessing-bucket/*"
        }
    ]
} ]
}
```

✅ **Replace the following:**

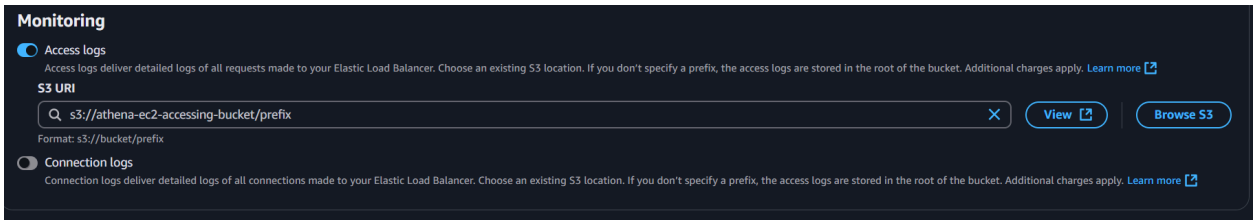
- `127311923021` → **ALB account ID**
- `arn:aws:s3:::athena-ec2-accessing-bucket/*` → **Your S3 ARN**

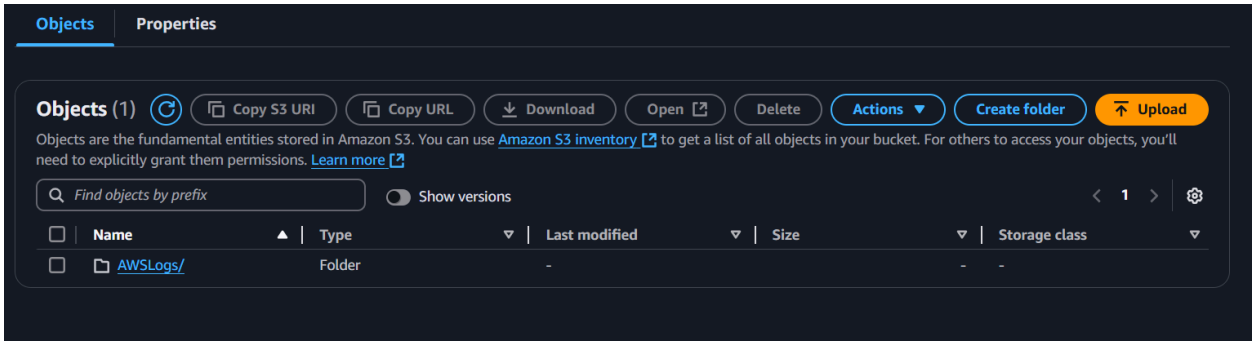
5. **Click Save**

Step 6: Enable ALB Logging to S3

To allow Application Load Balancer (ALB) to log traffic to your S3 bucket, you need to enable access logs and grant permissions.

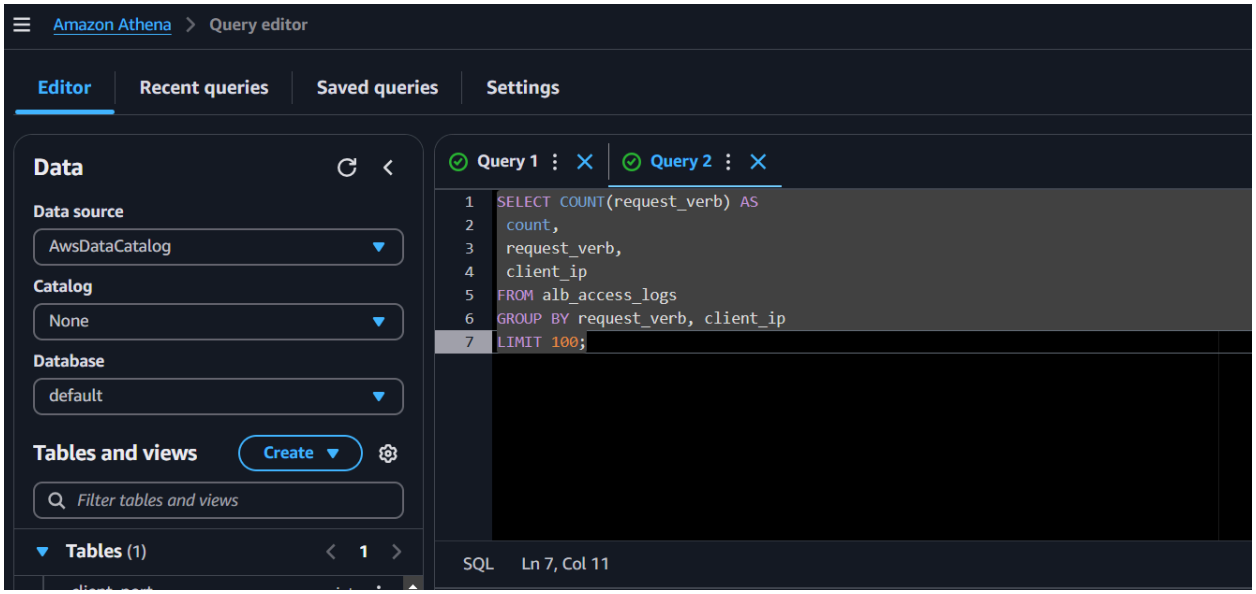
1. **Go to EC2 Dashboard → Click Load Balancers**
2. **Select Your ALB**
3. **Click Edit Attributes**
4. **Enable Access Logs**
5. **S3 Bucket Name: Enter `my-alb-logs-bucket`**
6. **Prefix (Optional): Enter `alb-logs/`**
7. **Click Save Changes**

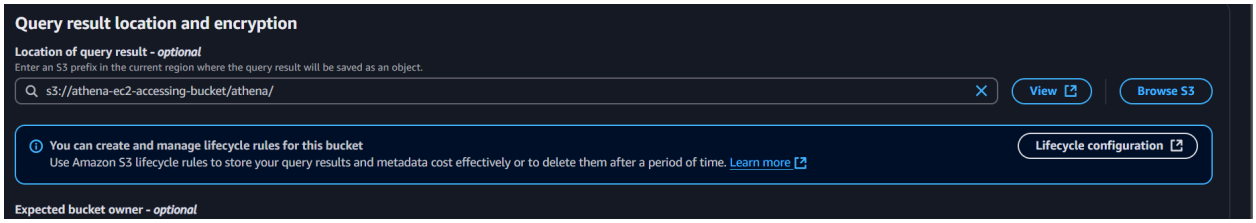




Step 7: Analyze ALB Logs Using AWS Athena

1. **Go to the AWS Athena Console**
2. Open the **Query Editor**
3. Run the following SQL command to create a database for ALB logs:
4. Goto setting
5. Click on manage
6. Add query result location

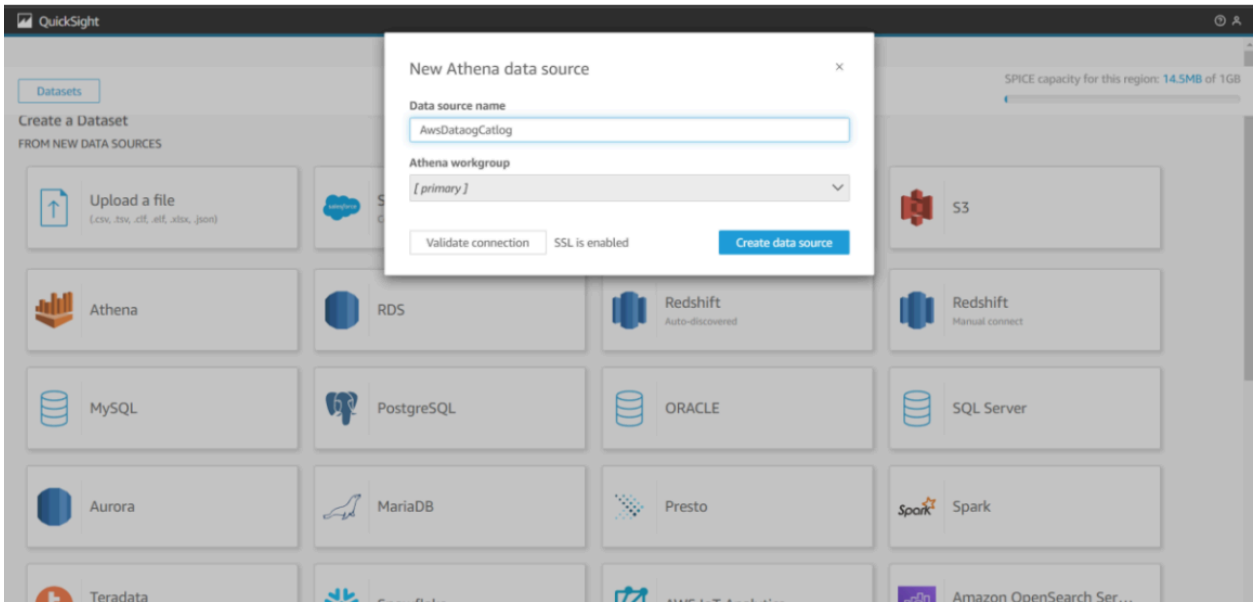


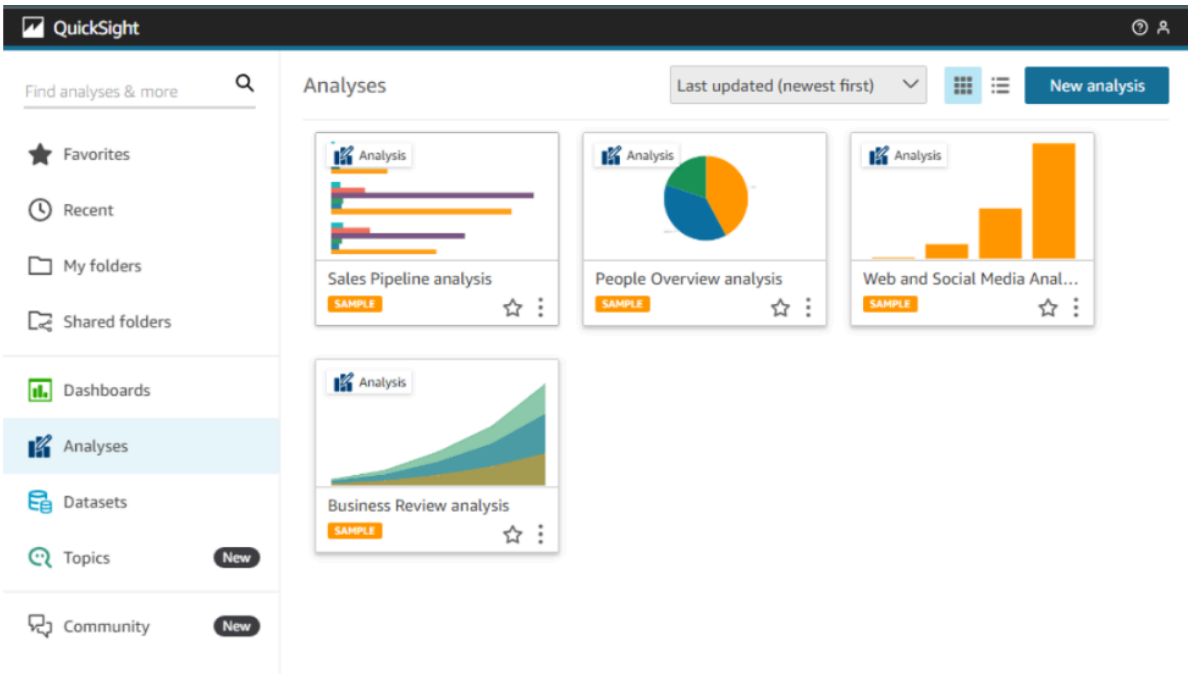


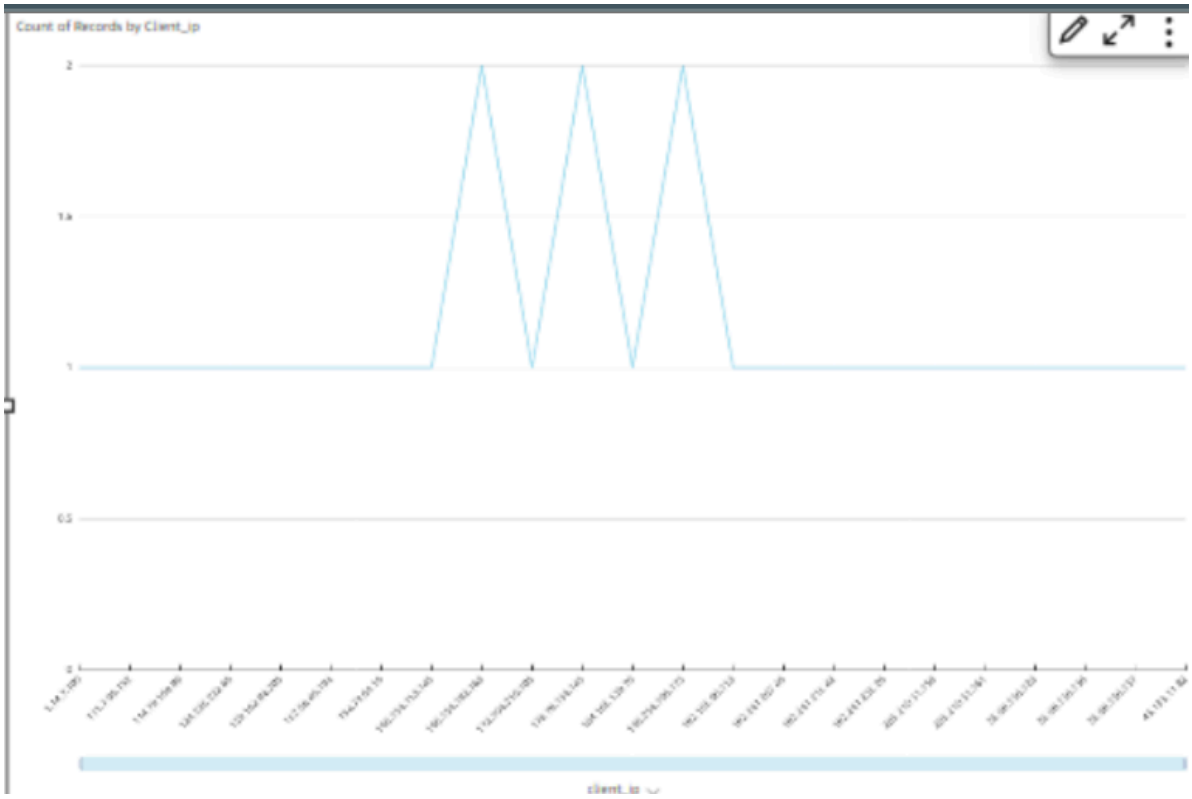
Step 8: Visualize ALB Logs in Amazon QuickSight

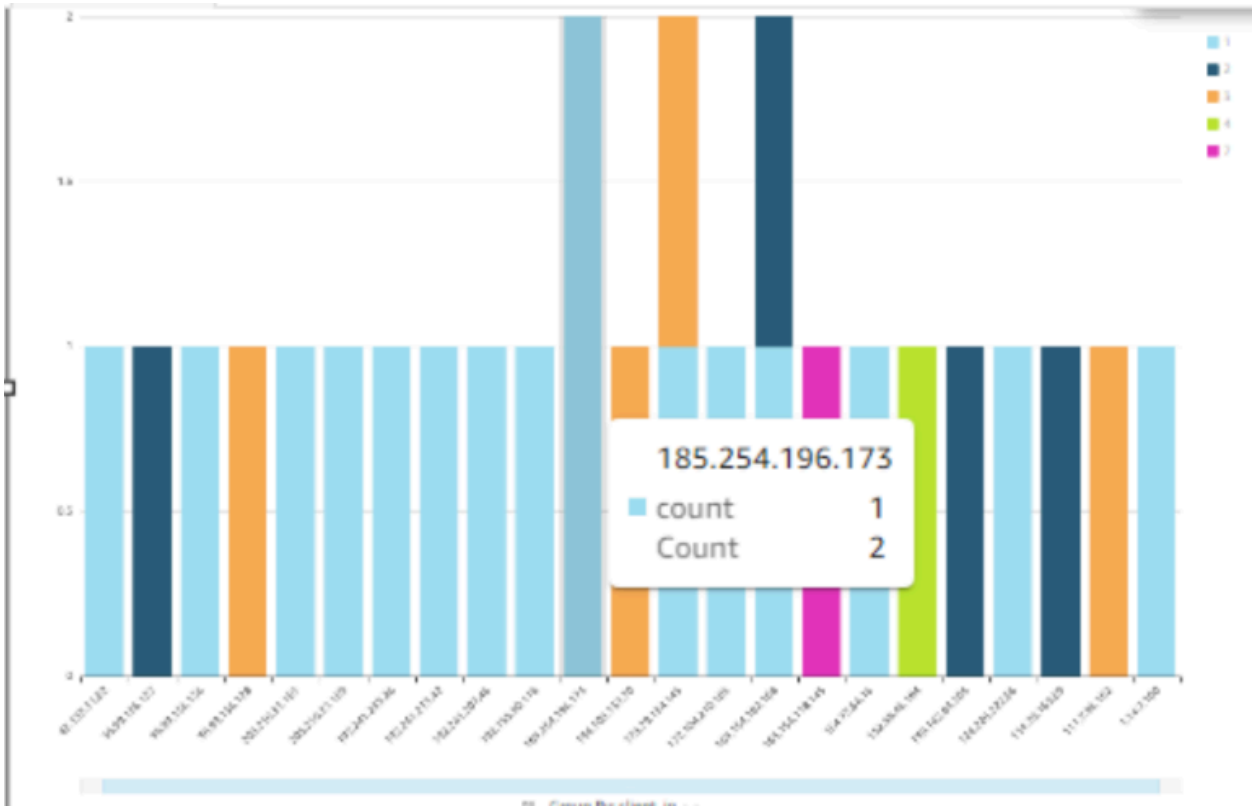
📌 Step 8.1: Enable Amazon QuickSight to Access Athena & S3

1. **Go to AWS QuickSight Console** → QuickSight
2. Navigate to New Analysis > New dataset > Athena
3. Click on create data source
4. Select the Y-axis dimension and Group/Color dimension


QuickSight
Datasets
Create a Dataset
FROM NEW DATA SOURCES
SPICE capacity for this region: 14.5MB of 1GB
New Athena data source
Data source name
AwsDataogCatlog
Athena workgroup
[primary]
Validate connection
SSL is enabled
Create data source
Upload a file
S3
Athena
RDS
Redshift
Auto-discovered
Redshift
Manual connect
MySQL
PostgreSQL
ORACLE
SQL Server
Aurora
MariaDB
Presto
Spark
Teradata


QuickSight
Find analyses & more
Favorites
Recent
My folders
Shared folders
Dashboards
Analyses
Datasets
Topics
New
Community
New
Analyses
Last updated (newest first)
New analysis
Analysis
Sales Pipeline analysis
SAMPLE
Analysis
People Overview analysis
SAMPLE
Analysis
Web and Social Media Anal...
SAMPLE
Analysis
Business Review analysis
SAMPLE





In this way you can use the Amazon Quick sight Analysis for Analysing the overall tasks.