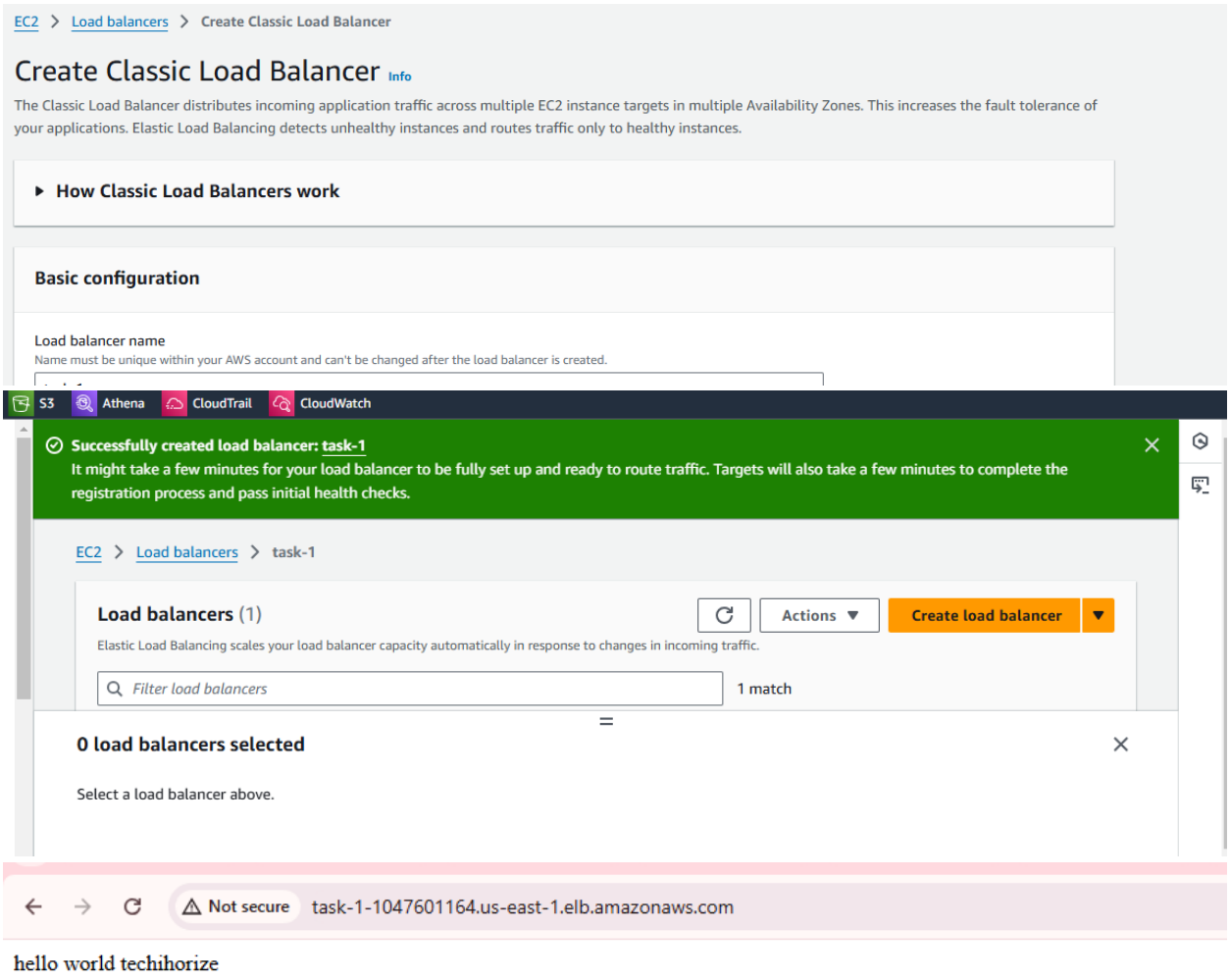
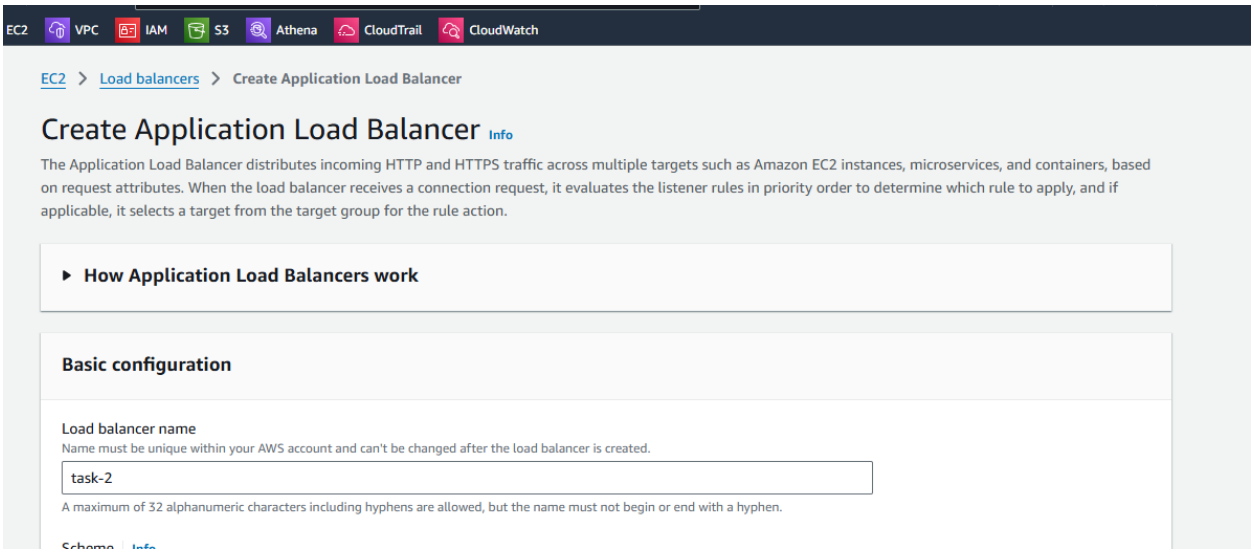
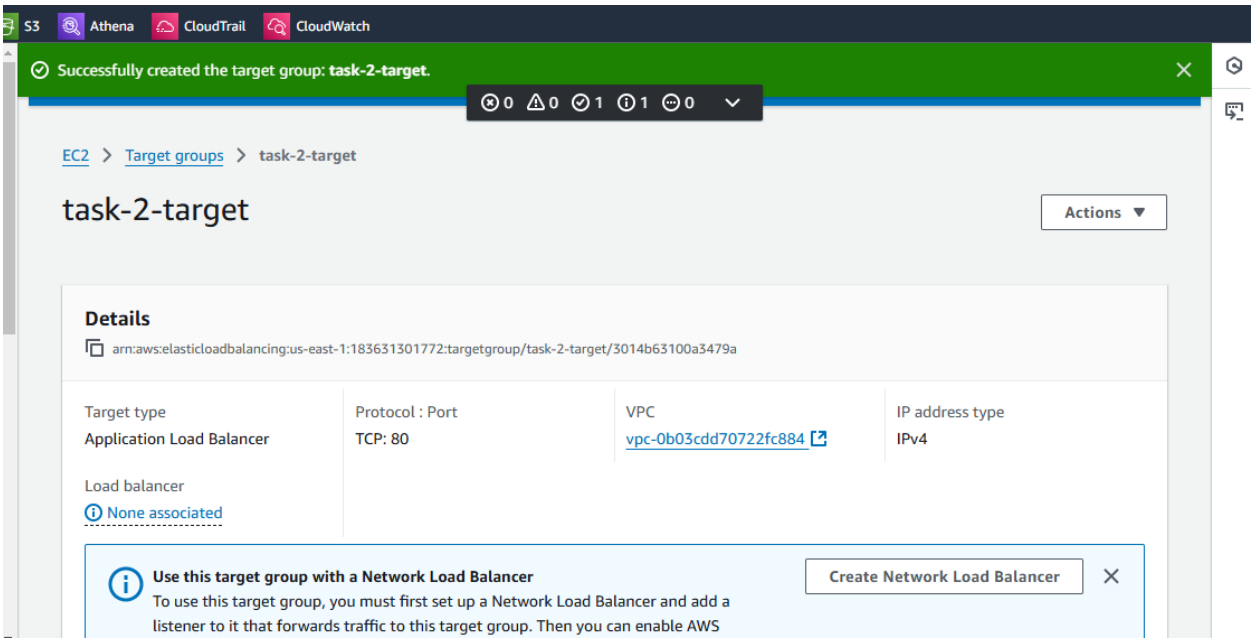
Load balancer Tasks

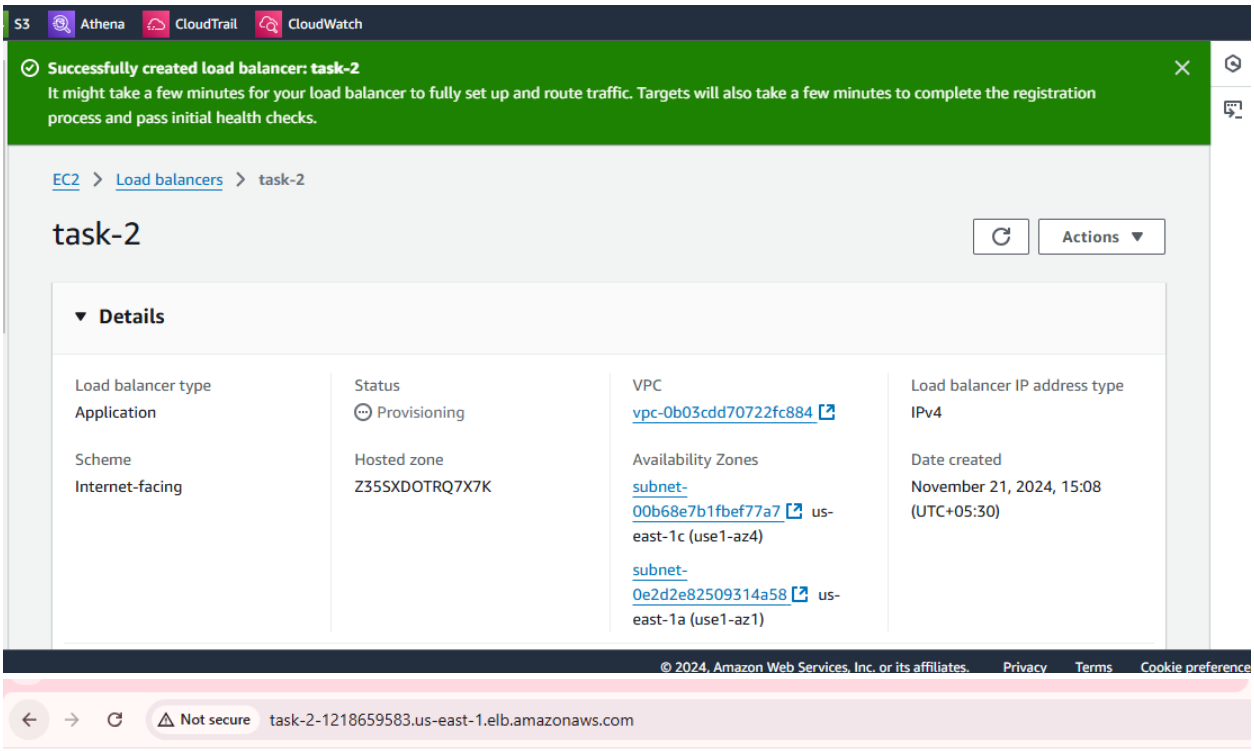
1) Configure Classic Load balancer.



2) Configure Application Load balancer.

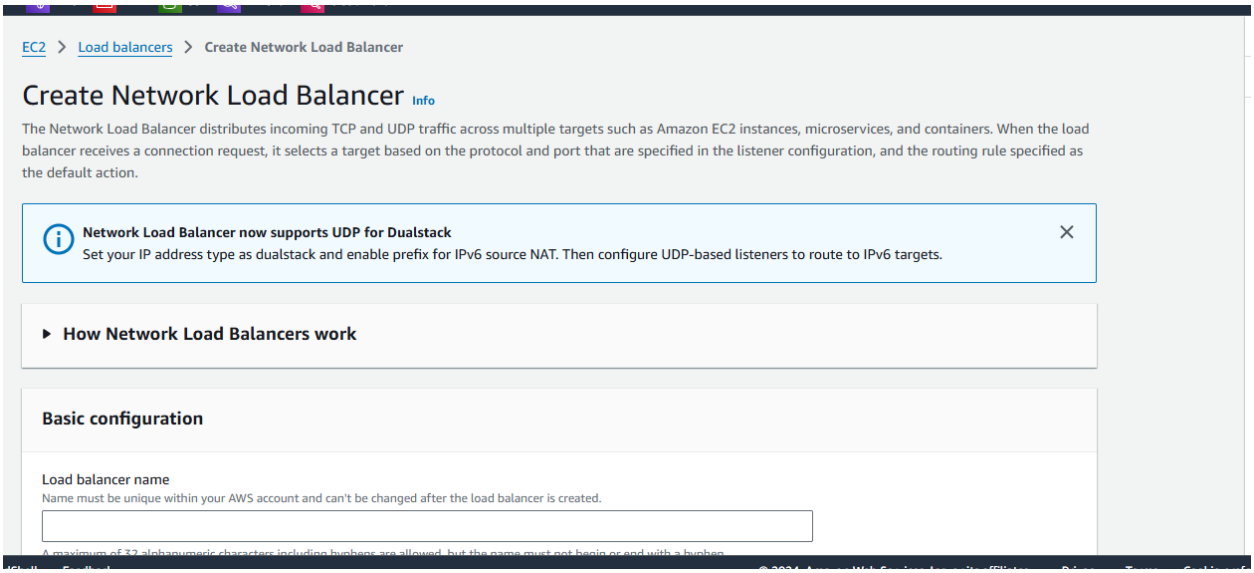

EC2
VPC
IAM
S3
Athena
CloudTrail
CloudWatch
EC2 > Load balancers > Create Application Load Balancer
Create Application Load Balancer Info
The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based 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.
task-2
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

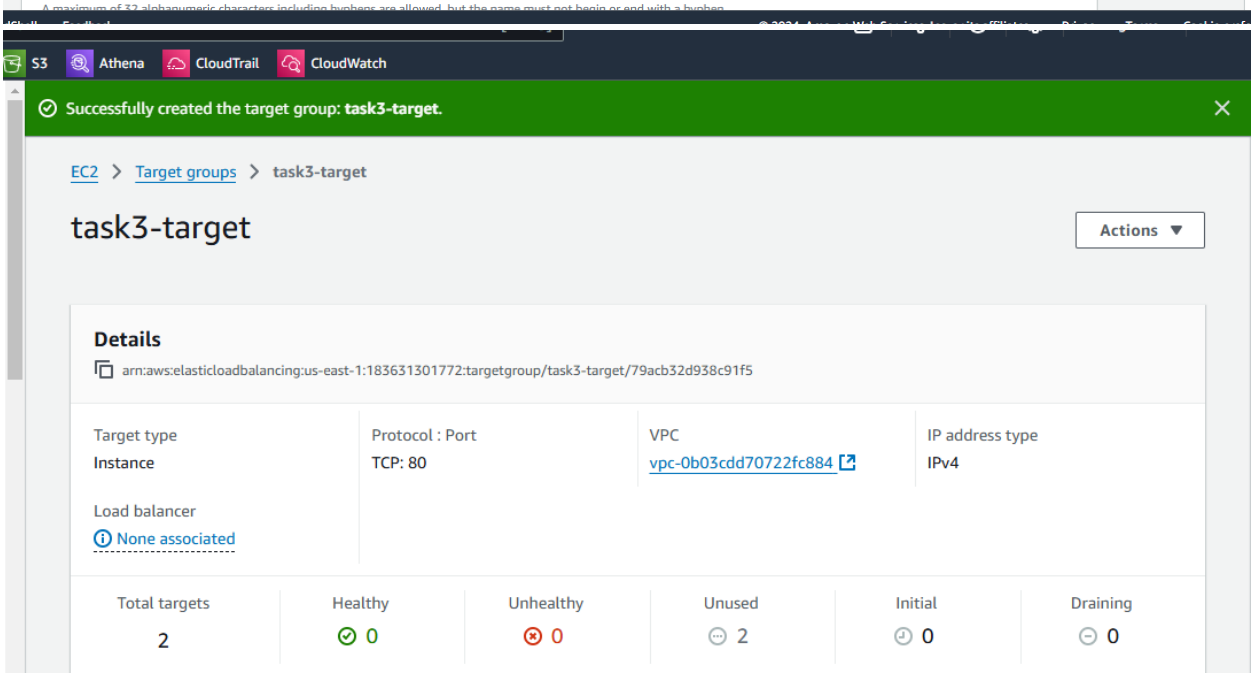

S3
Athena
CloudTrail
CloudWatch
Successfully created the target group: task-2-target.
0 0 1 1 0
EC2 > Target groups > task-2-target
task-2-target
Actions
Details
arn:aws:elasticloadbalancing:us-east-1:183631301772:targetgroup/task-2-target/3014b63100a3479a
Target type
Application Load Balancer
Protocol : Port
TCP: 80
VPC
vpc-0b03cdd70722fc884
IP address type
IPv4
Load balancer
None associated
Use this target group with a Network Load Balancer
To use this target group, you must first set up a Network Load Balancer and add a listener to it that forwards traffic to this target group. Then you can enable AWS
Create Network Load Balancer

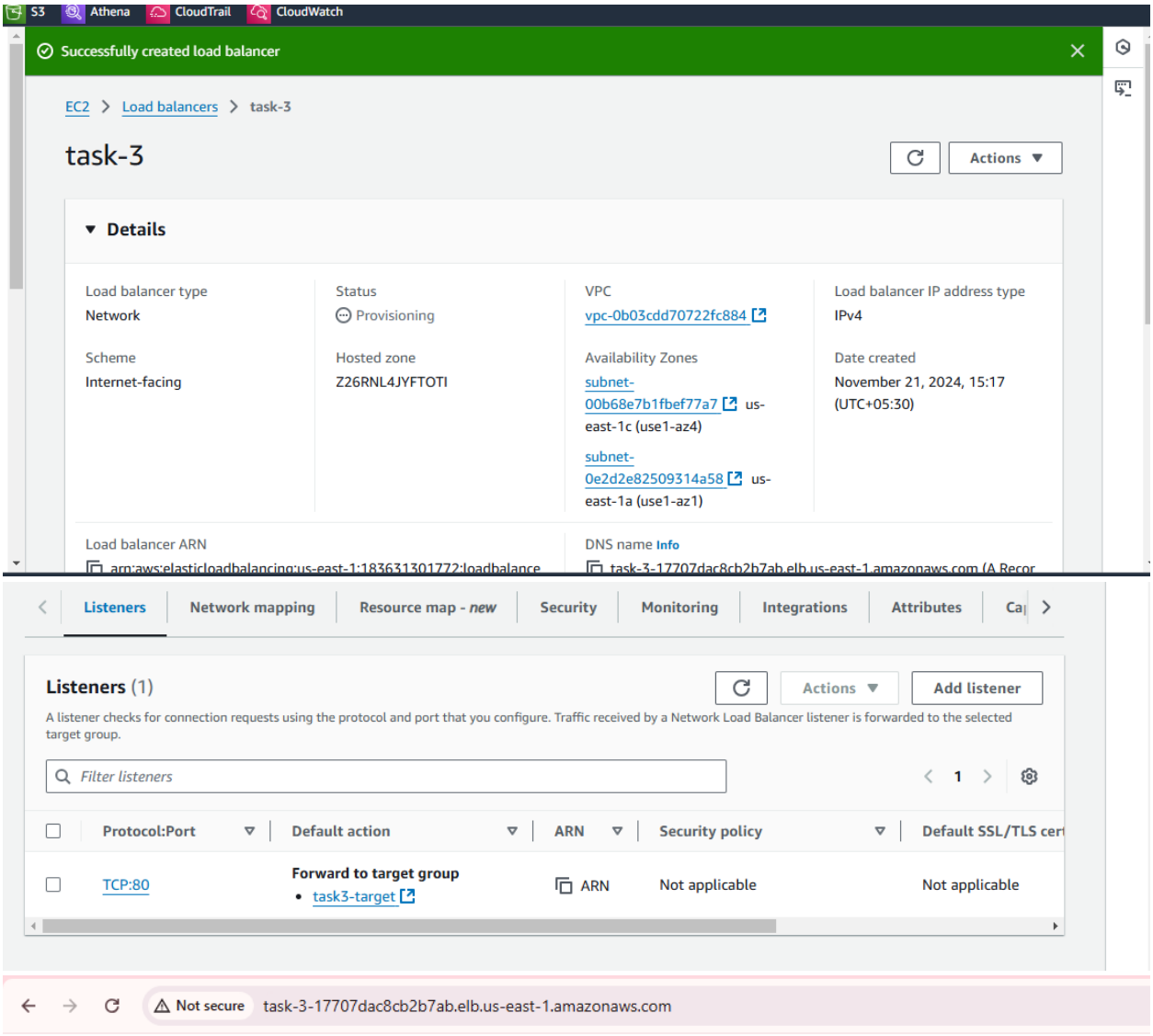


hello world techihorize

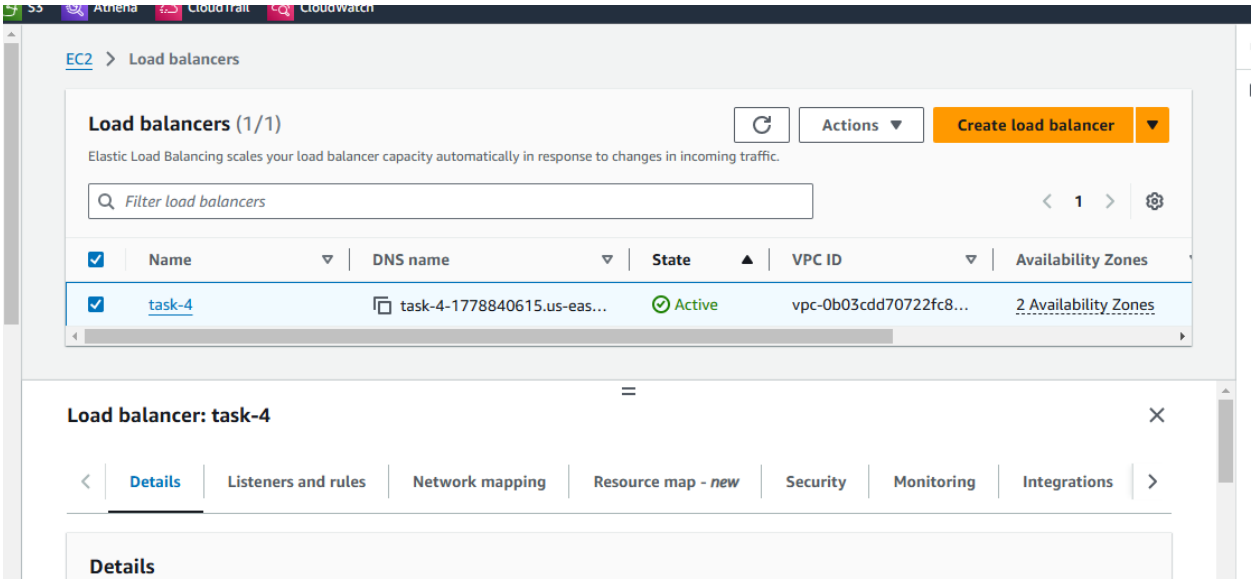
3) Configure Network Load balancer.

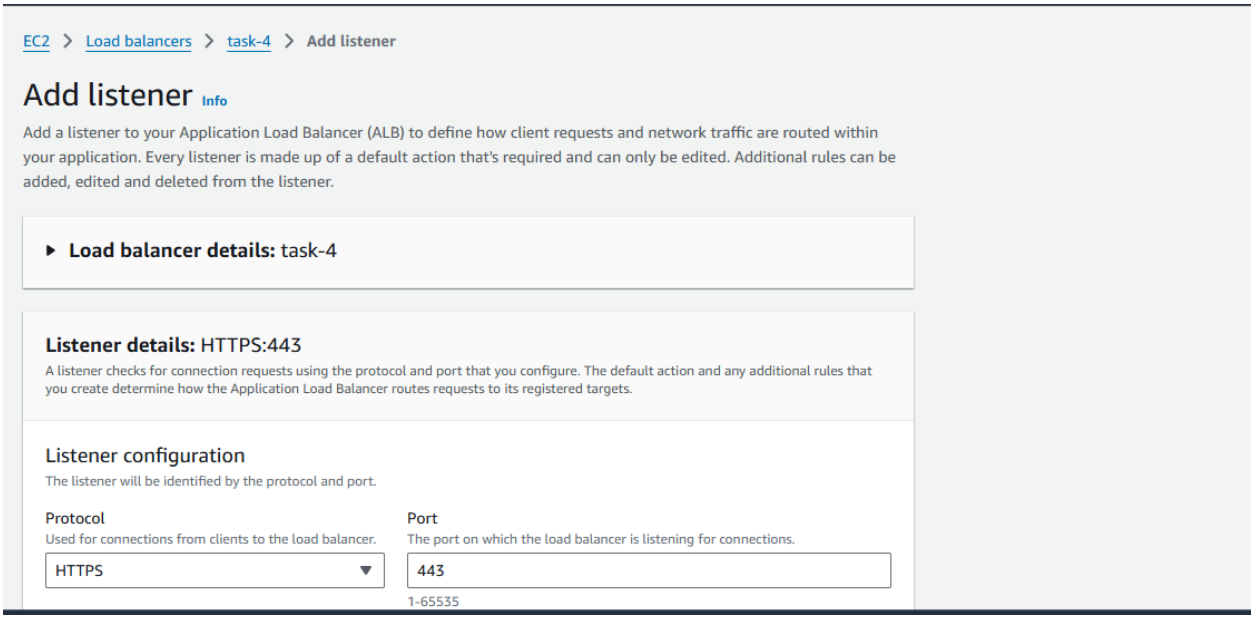

EC2 > Load balancers > Create Network Load Balancer
Create Network Load Balancer Info
The Network Load Balancer distributes incoming TCP and UDP traffic across multiple targets such as Amazon EC2 instances, microservices, and containers. When the load balancer receives a connection request, it selects a target based on the protocol and port that are specified in the listener configuration, and the routing rule specified as the default action.
Network Load Balancer now supports UDP for Dualstack
Set your IP address type as dualstack and enable prefix for IPv6 source NAT. Then configure UDP-based listeners to route to IPv6 targets.
How Network 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.

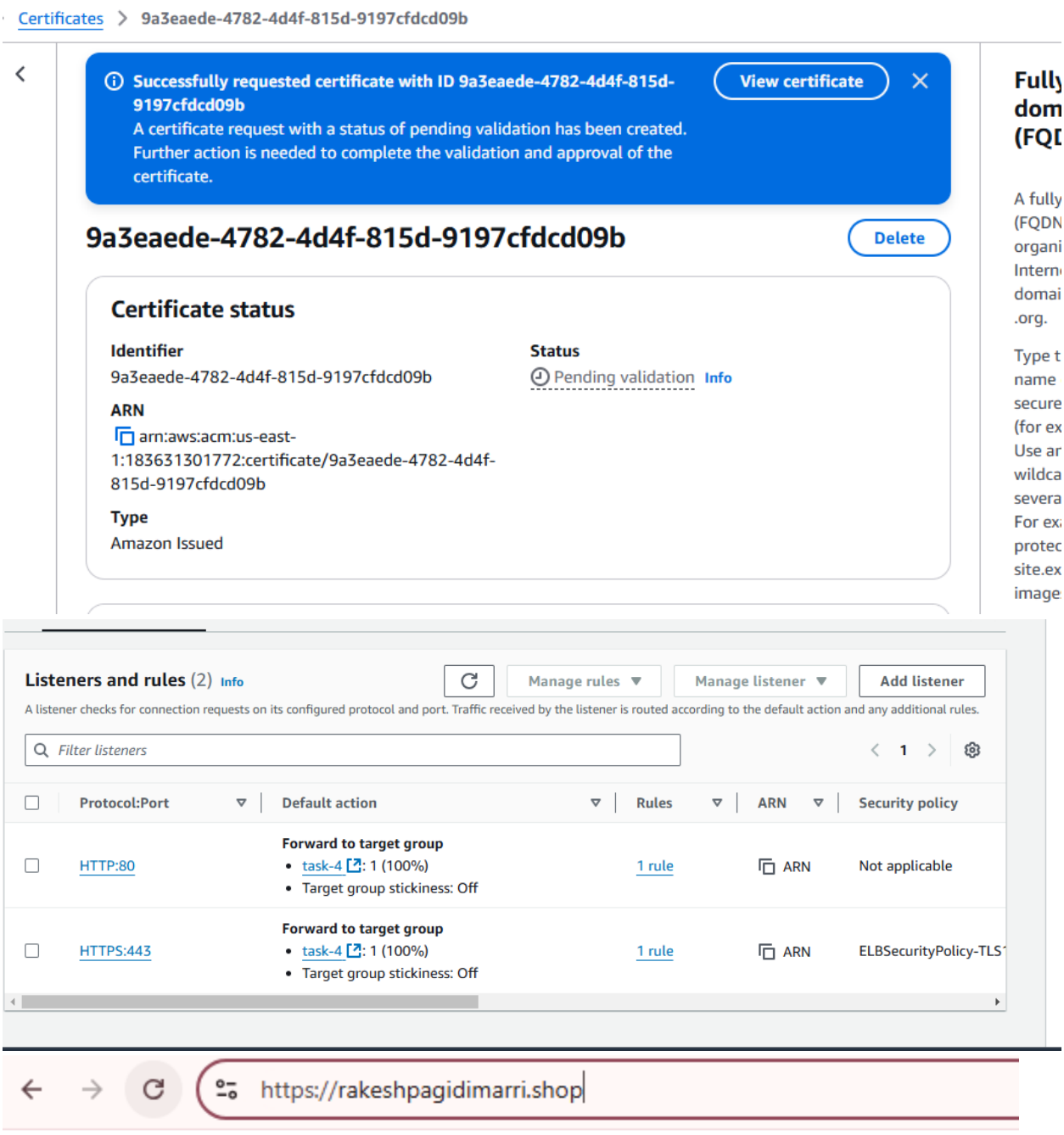

S3
Athena
CloudTrail
CloudWatch
Successfully created the target group: task3-target.
EC2 > Target groups > task3-target
task3-target
Actions
Details
arn:aws:elasticloadbalancing:us-east-1:183631301772:targetgroup/task3-target/79acb32d938c91f5
Target type
Instance
Protocol : Port
TCP: 80
VPC
vpc-0b03cdd70722fc884
IP address type
IPv4
Load balancer
None associated
Total targets
2
Healthy
0
Unhealthy
0
Unused
2
Initial
0
Draining
0



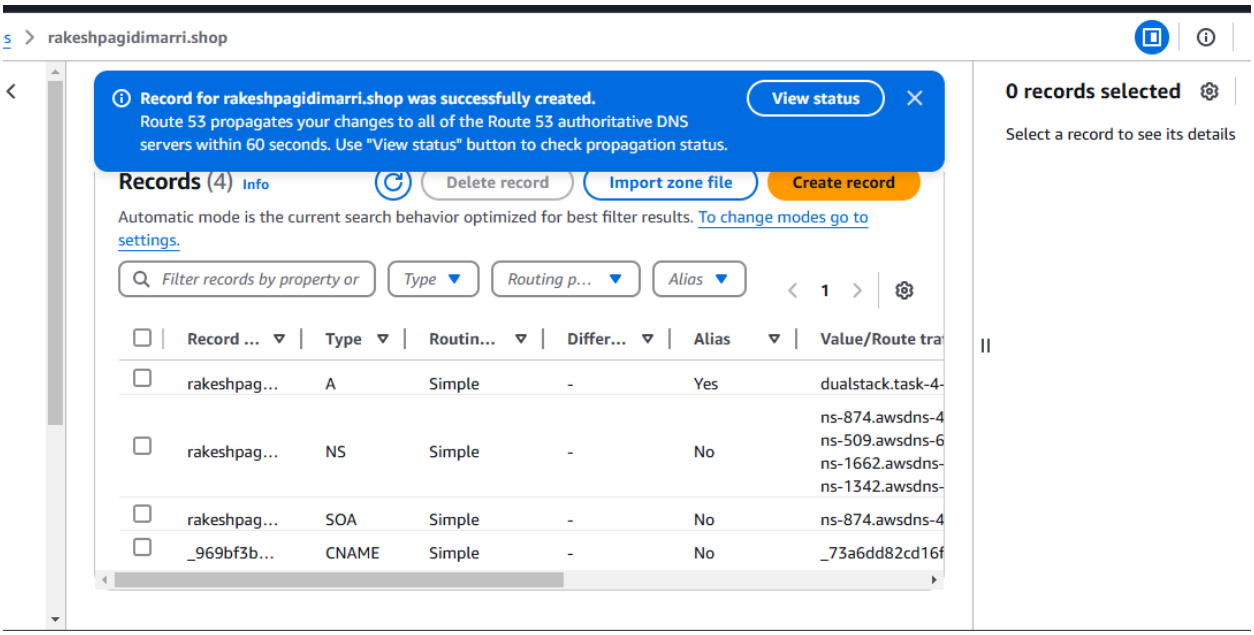
4) Attach SSL for application load balancer.


S3
Athena
CloudTrail
CloudWatch
EC2 > Load balancers
Load balancers (1/1)
Actions
Create load balancer
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
task-4
task-4-1778840615.us-eas...
Active
vpc-0b03cdd70722fc8...
2 Availability Zones
Load balancer: task-4
Details
Listeners and rules
Network mapping
Resource map - new
Security
Monitoring
Integrations
Details

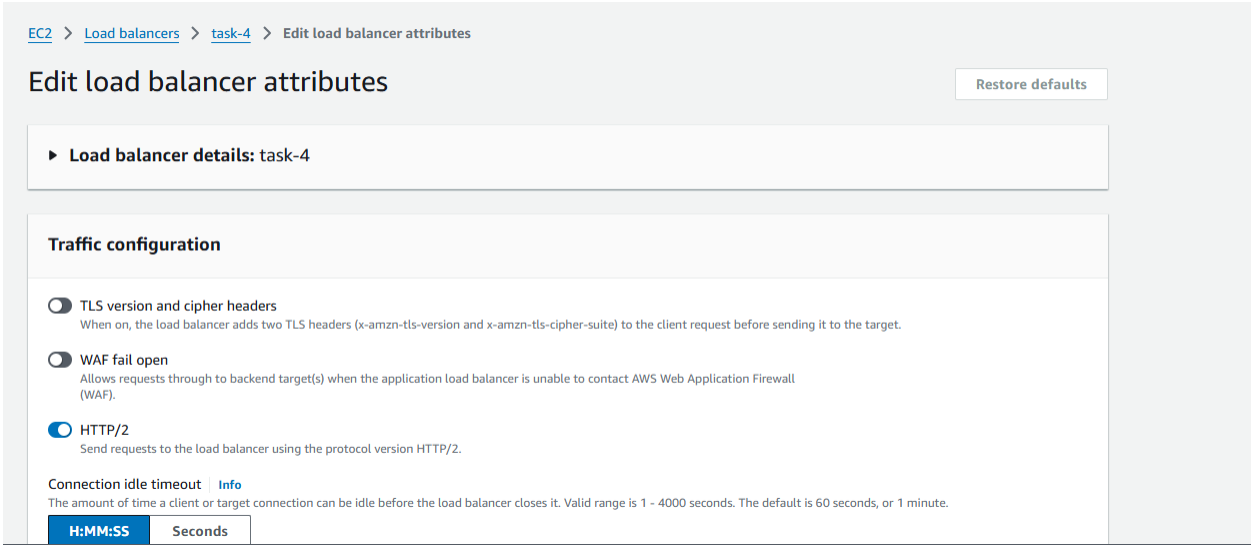

EC2 > Load balancers > task-4 > Add listener
Add listener Info
Add a listener to your Application Load Balancer (ALB) to define how client requests and network traffic are routed within your application. Every listener is made up of a default action that's required and can only be edited. Additional rules can be added, edited and deleted from the listener.
Load balancer details: task-4
Listener details: HTTPS:443
A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.
Listener configuration
The listener will be identified by the protocol and port.
Protocol
Used for connections from clients to the load balancer.
HTTPS
Port
The port on which the load balancer is listening for connections.
443
1-65535

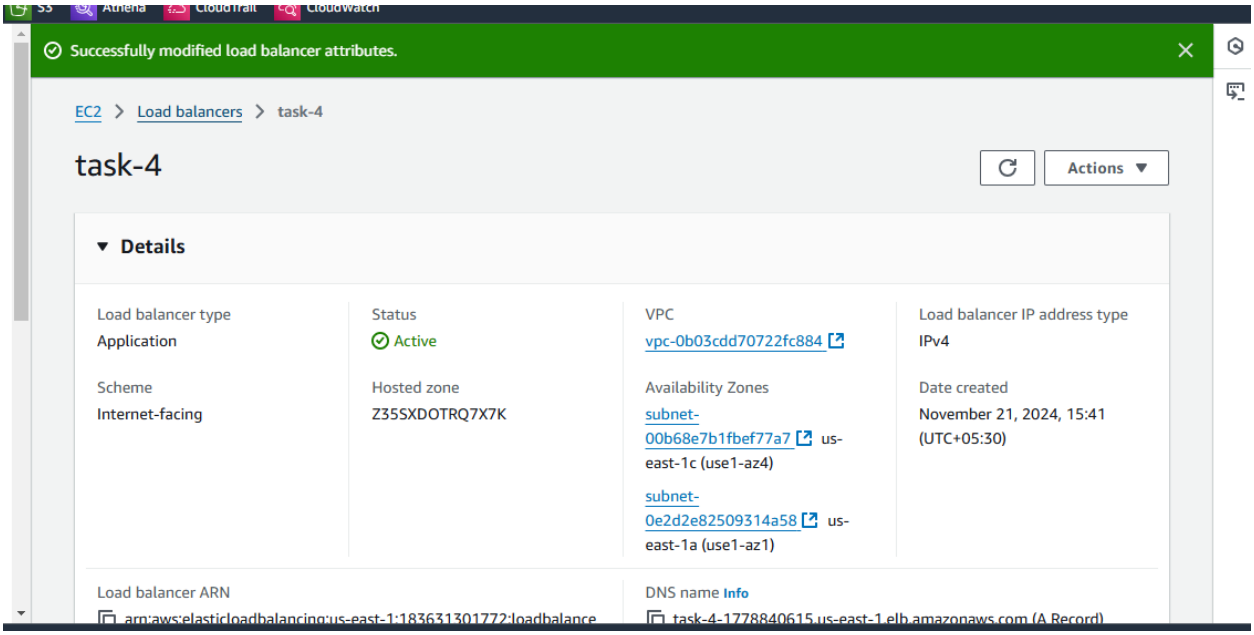


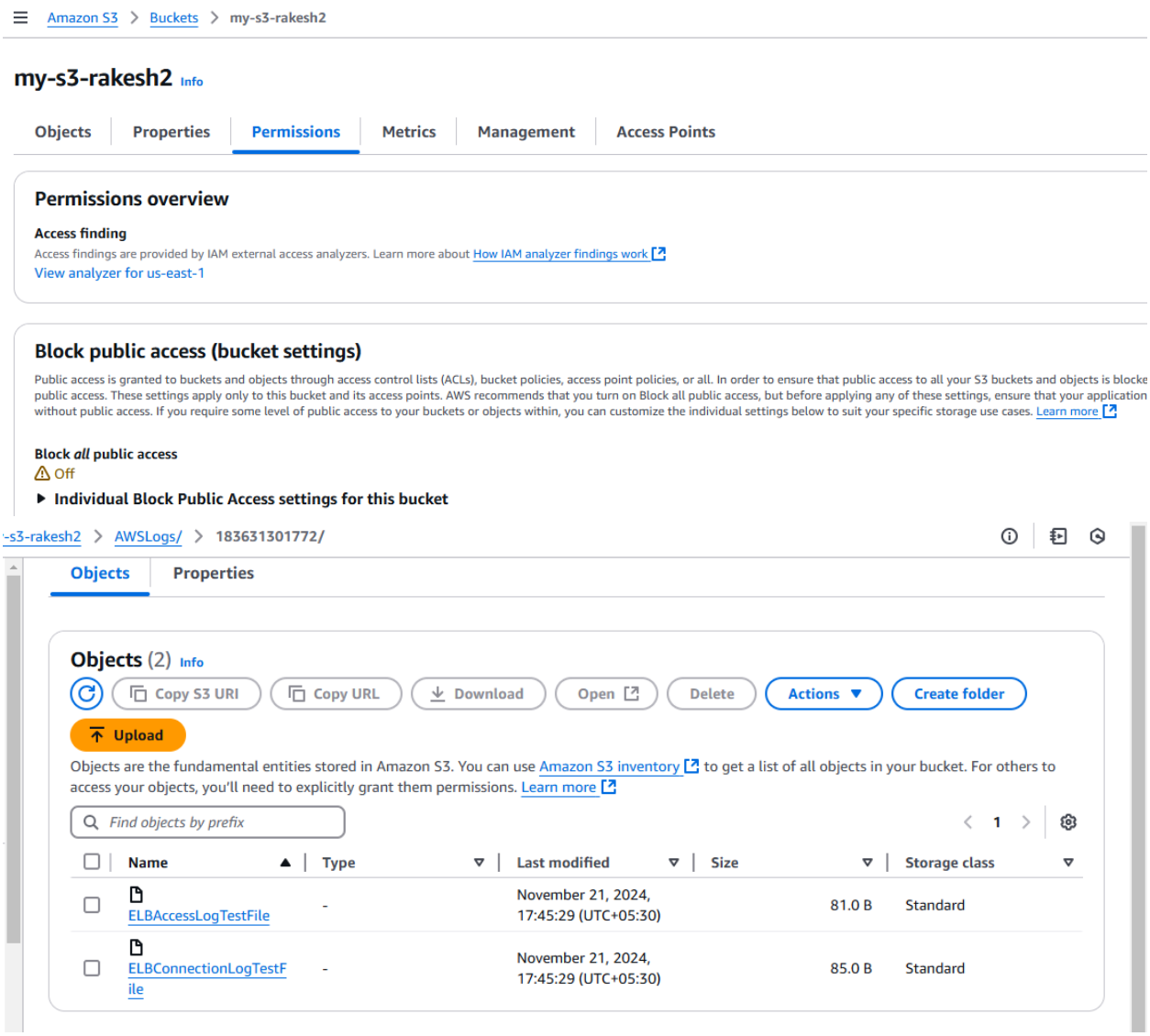
5) Map Applciation load balancer to R53.



6) Push the application load balancer logs to s3.




S3
Athena
CloudTrail
CloudWatch
Successfully modified load balancer attributes.
EC2 > Load balancers > task-4
task-4
Actions
Details
Load balancer type
Application
Status
Active
VPC
vpc-0b03cdd70722fc884
Load balancer IP address type
IPv4
Scheme
Internet-facing
Hosted zone
Z35SXDOTRQ7X7K
Availability Zones
subnet-00b68e7b1fbef77a7 us-east-1c (use1-az4)
subnet-0e2d2e82509314a58 us-east-1a (use1-az1)
Date created
November 21, 2024, 15:41 (UTC+05:30)
Load balancer ARN
DNS name Info


Amazon S3 > Buckets > my-s3-rakesh2
my-s3-rakesh2 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access finding
Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work
View analyzer for us-east-1
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocke
public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your application
without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Off
Individual Block Public Access settings for this bucket
-s3-rakesh2 > AWSLogs/ > 183631301772/
Objects
Properties
Objects (2) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to
access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
1
Name
Type
Last modified
Size
Storage class
ELBAccessLogTestFile
-
November 21, 2024, 17:45:29 (UTC+05:30)
81.0 B
Standard
ELBConnectionLogTestFile
-
November 21, 2024, 17:45:29 (UTC+05:30)
85.0 B
Standard