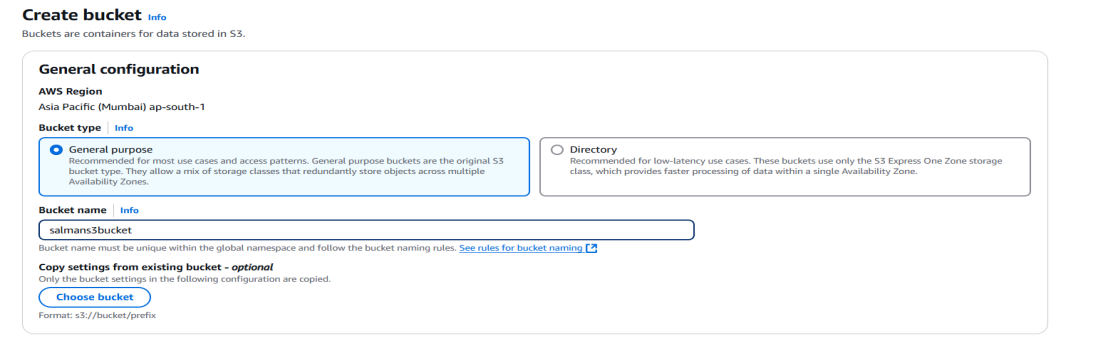
AWS Task-3

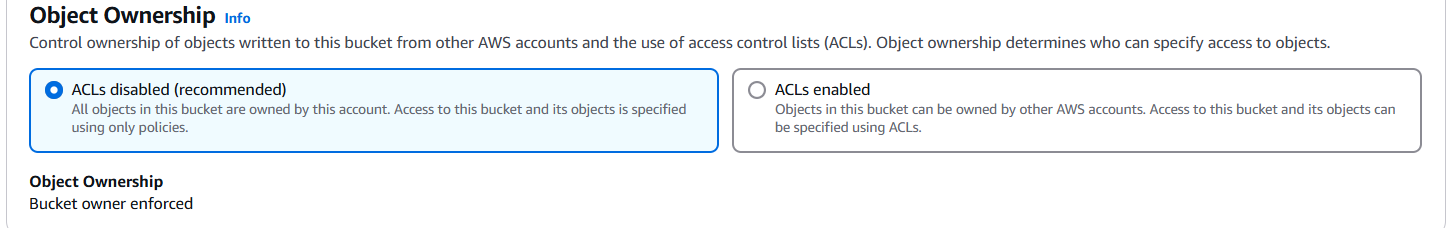
Create a S3 bucket, with no public access and upload files to the bucket & view the logs using cloudwatch for the uploaded files.

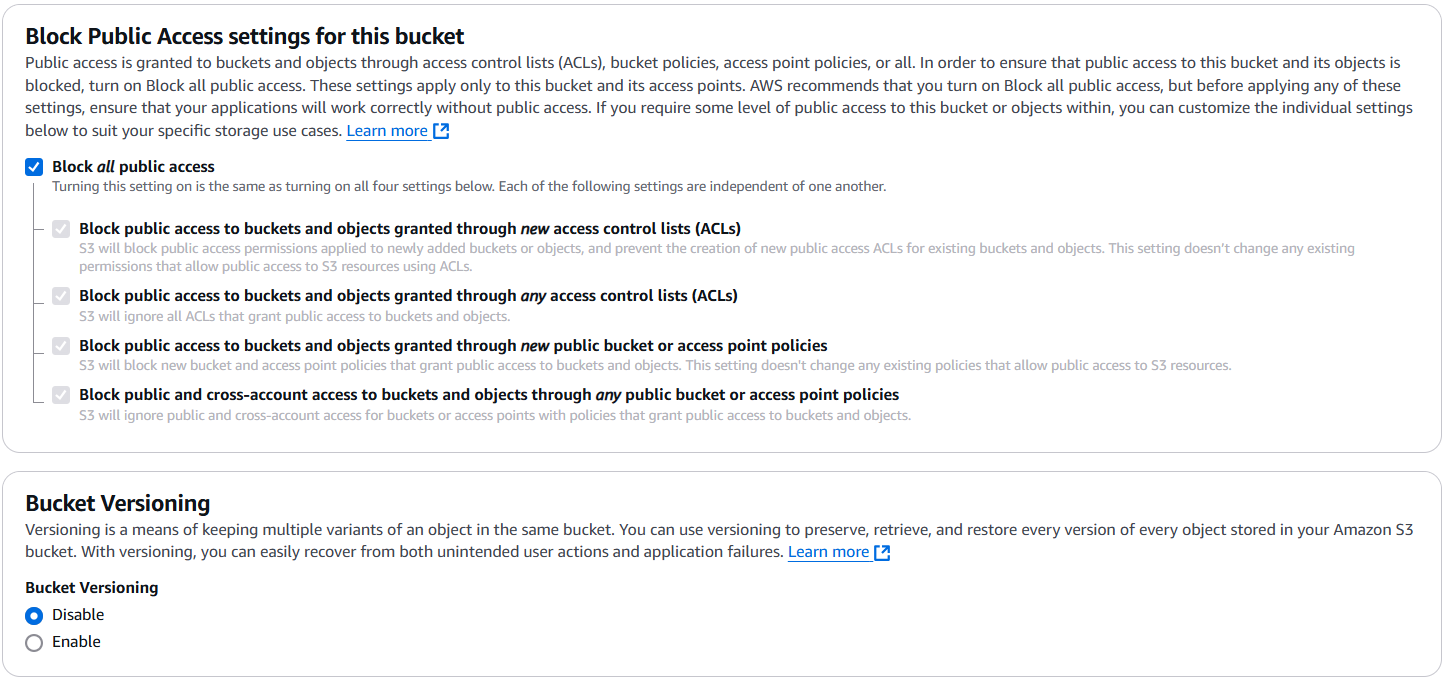
### ****1. Create an S3 Bucket with No Public Access****

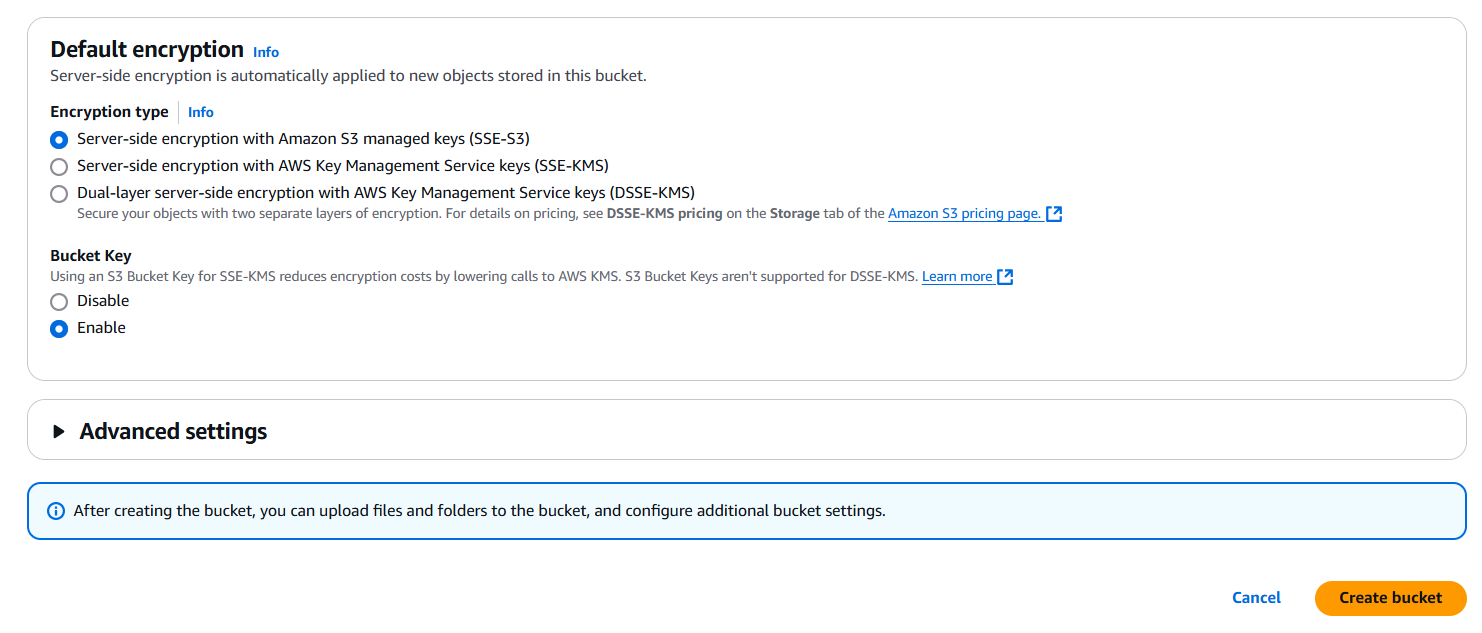
**Log in to AWS Management Console**.

* **Navigate to the S3 Service**:
* Go to "Services" > "S3".
* **Create a Bucket**:
* Click on **Create bucket**.
* Enter a unique bucket name (e.g.salmans3bucket).
* Select the desired AWS Region.
* **Block All Public Access**:
* Under "Block Public Access settings for this bucket," ensure all four options are checked:
* Block all public access.
* Block public ACLs.
* Ignore public ACLs.
* Block public bucket policies.
* Click **Create bucket**.



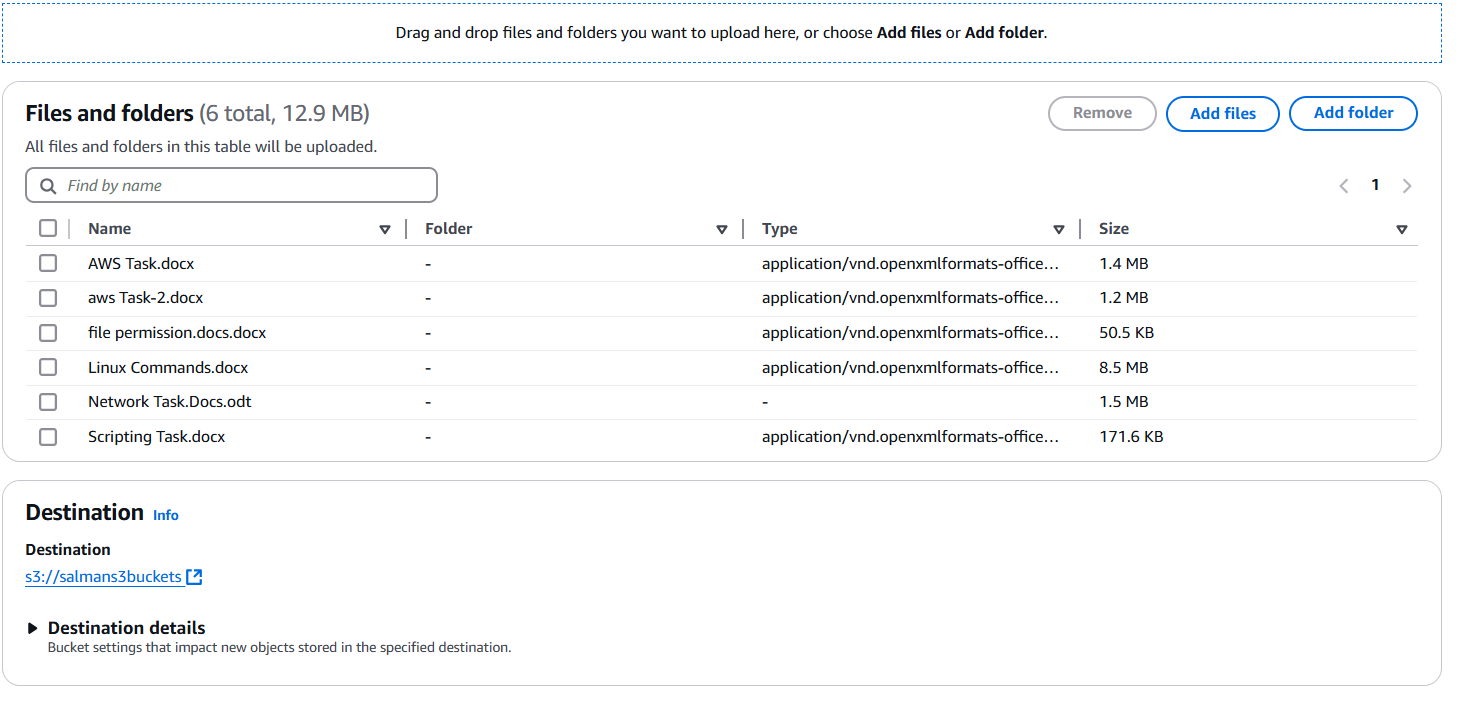


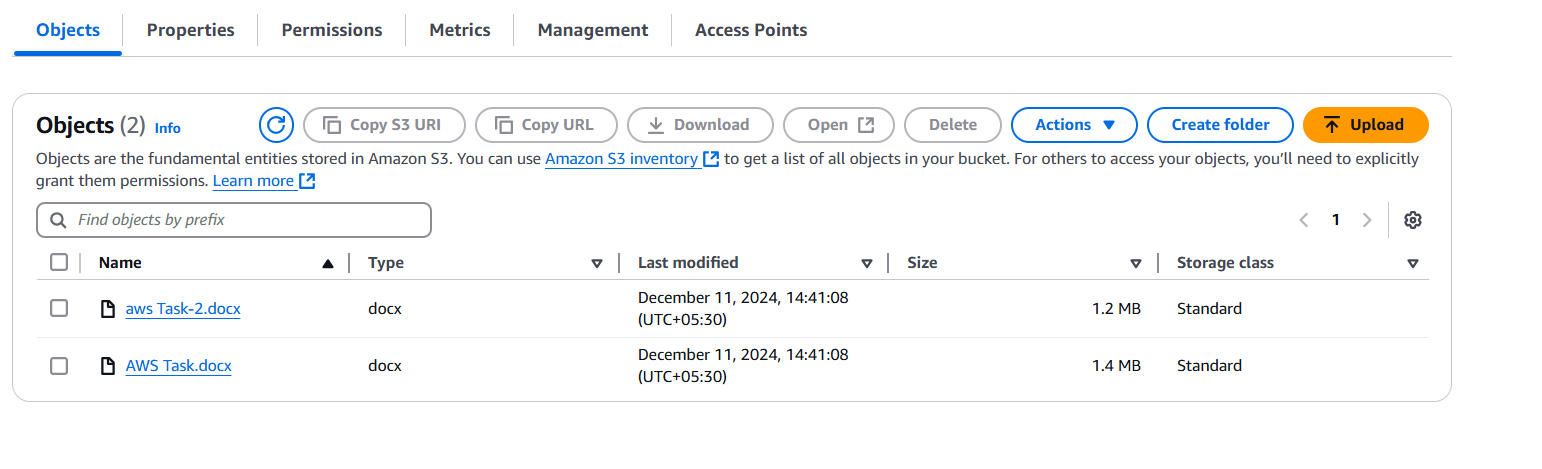




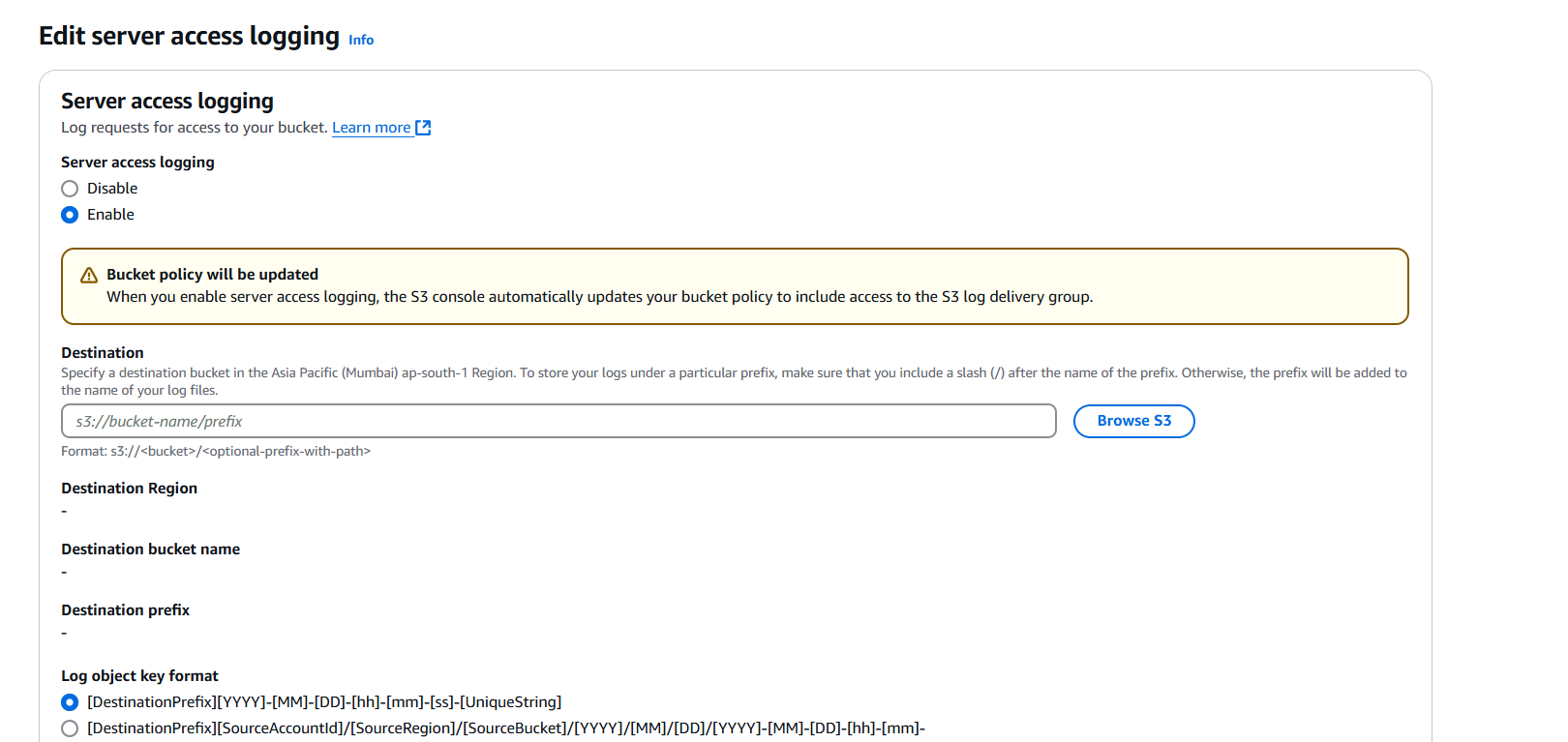
### ****2. Upload Files to the Bucket****

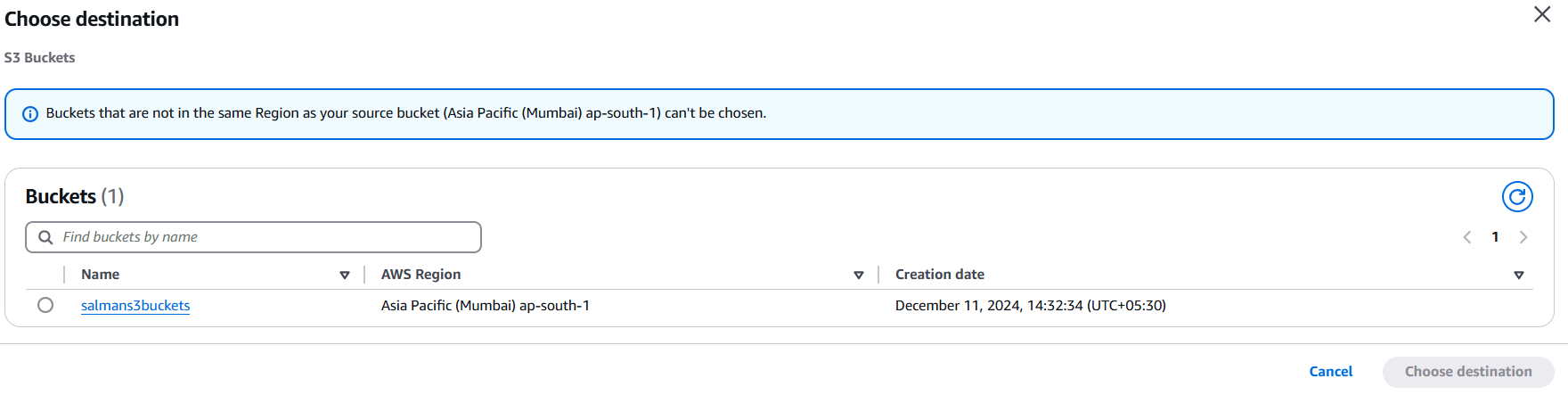
* **Select the Bucket**
* Open the created bucket from the S3 console.
* **Upload Files**:
* Click **Upload**.
* Drag and drop files or browse to select files.
* Click **Upload**.



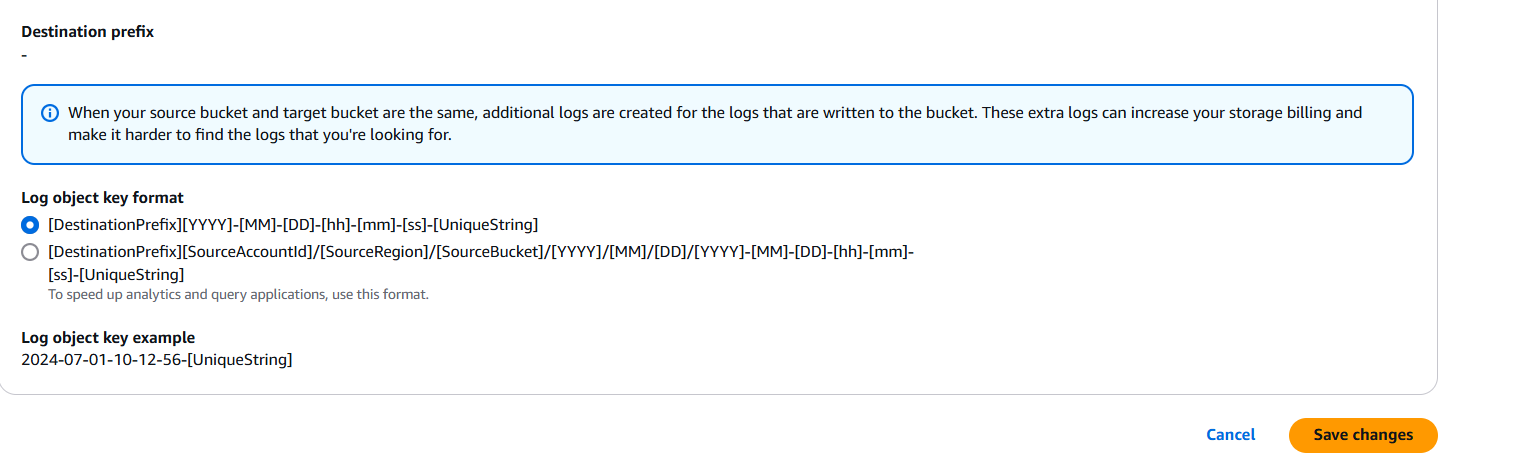
**3. Enable Logging for the Bucket**

* **Enable Server Access Logs**:
* Open the bucket properties.
* Under **Server access logging**, choose **Enable**.
* Select a target bucket for logs (create a separate bucket if needed, e.g., my-log-bucket).
* **Grant Logging Permissions**:
* Ensure the target bucket has a bucket policy granting write access for the logs.

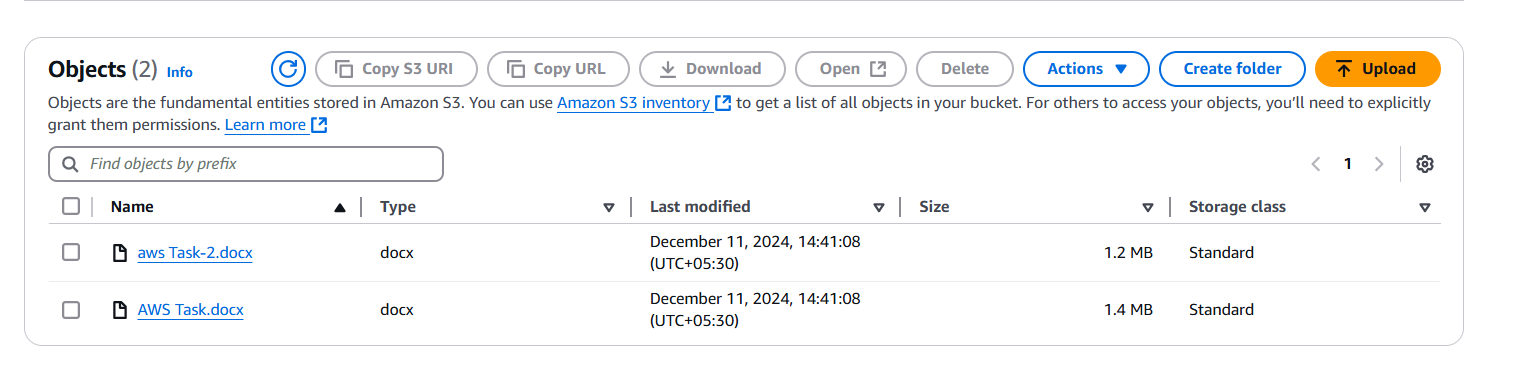


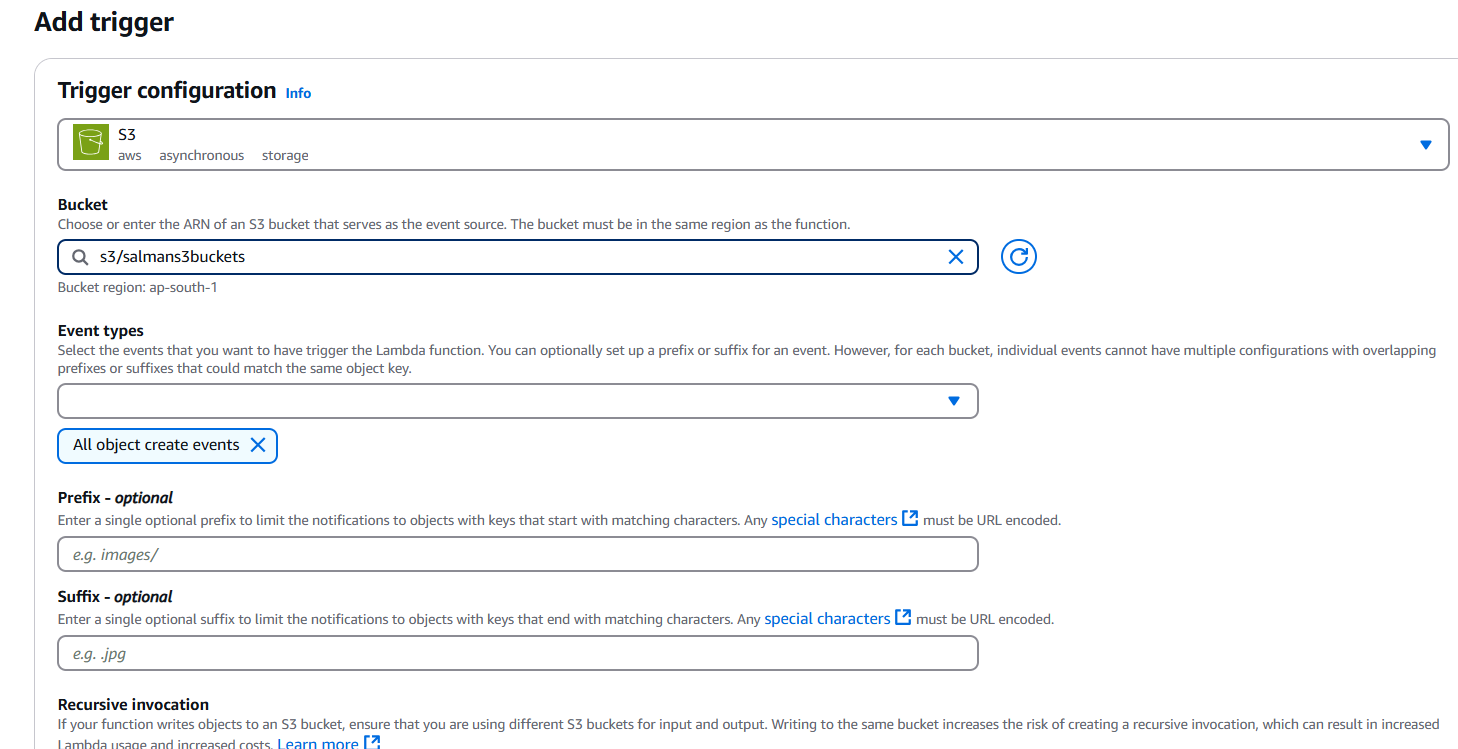
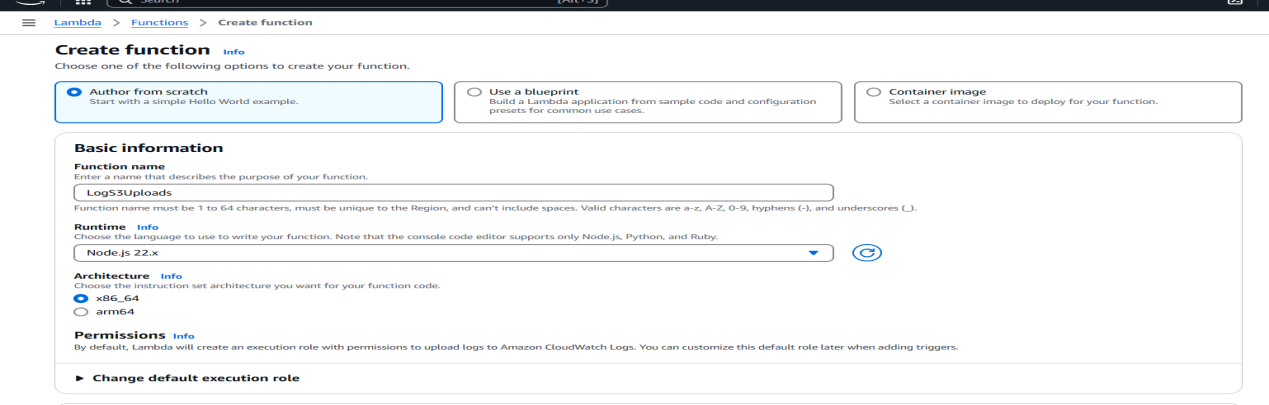


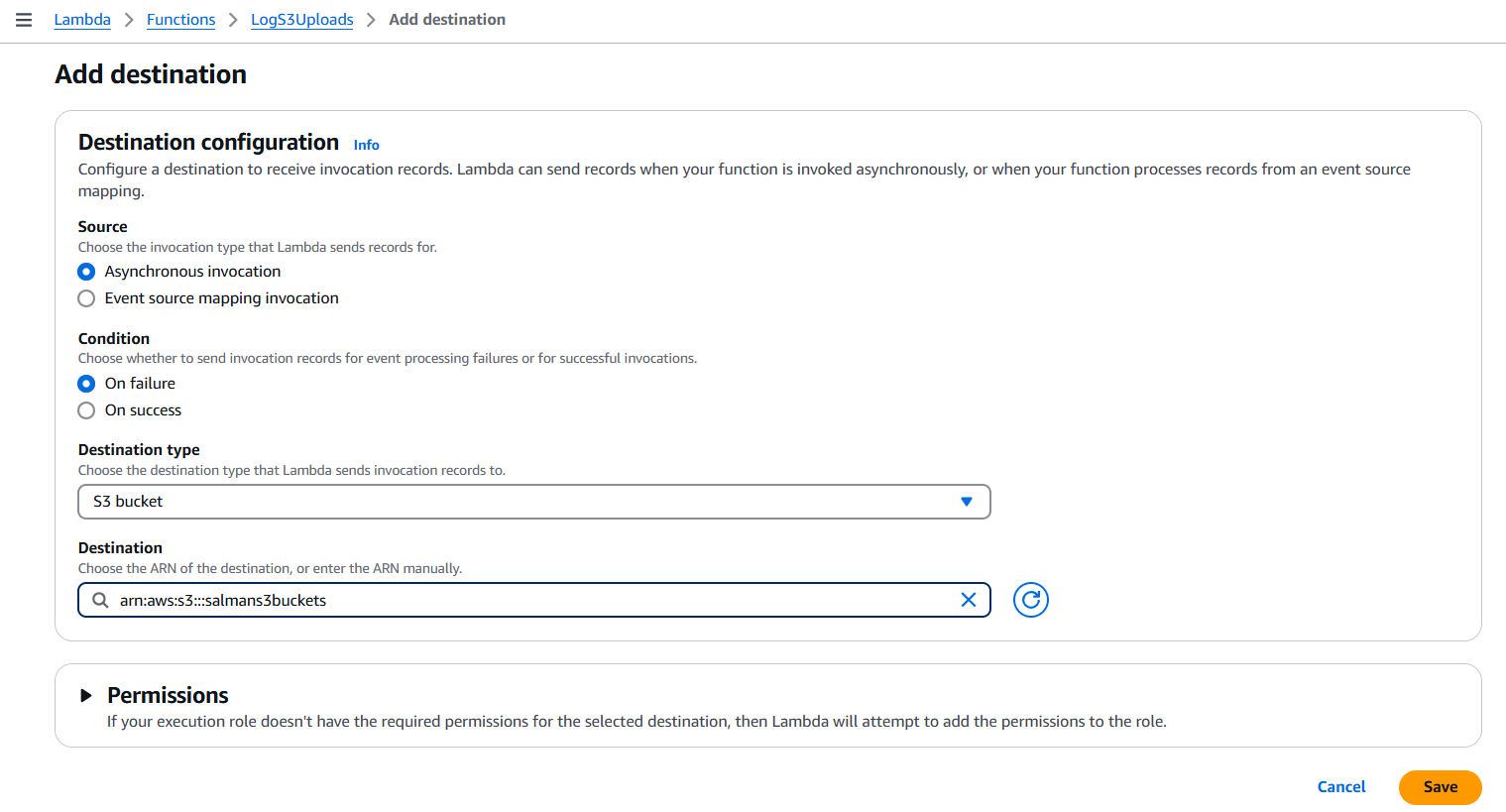


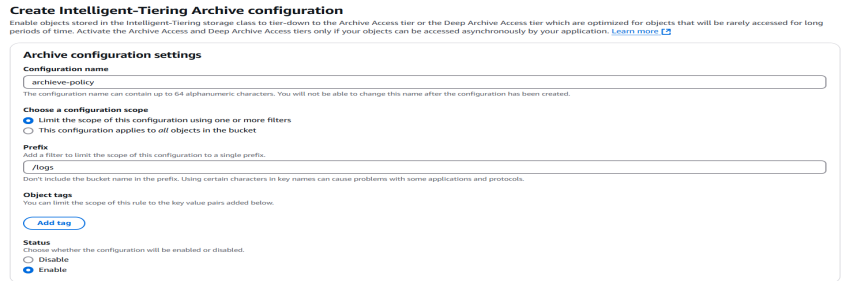


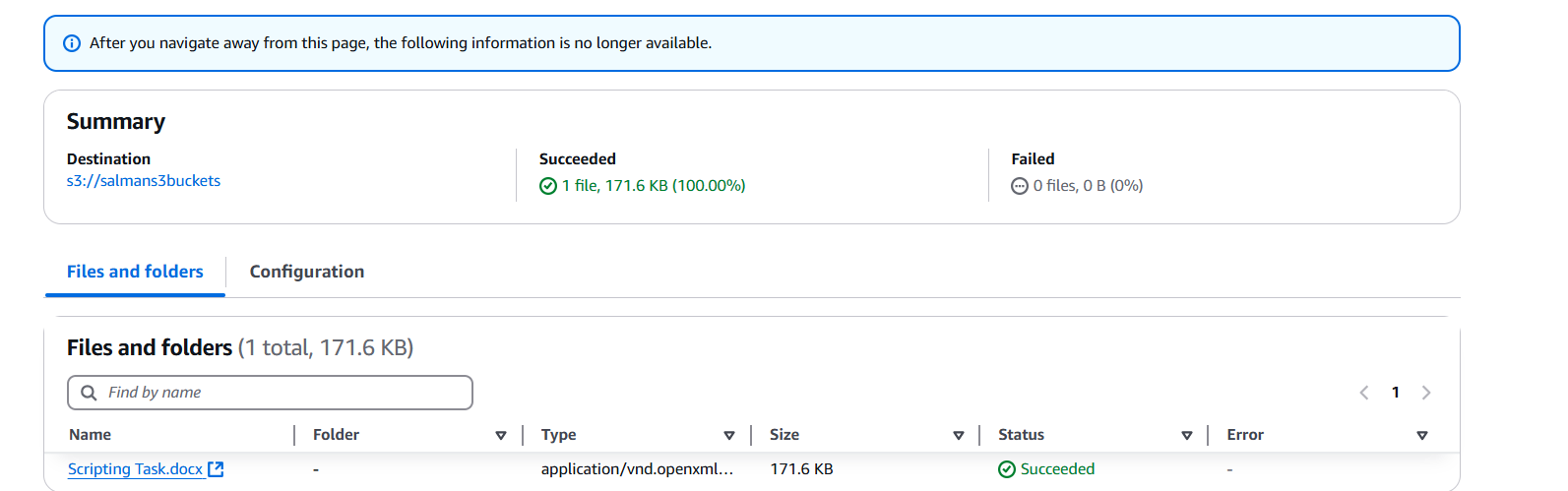
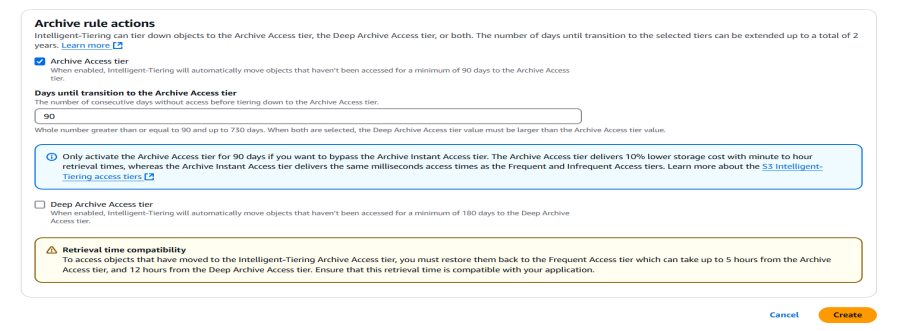
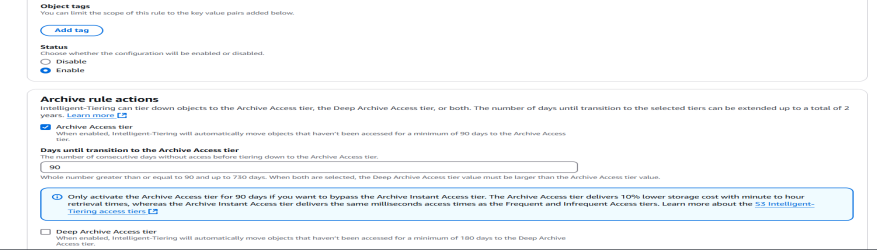
### ****4. View Logs in CloudWatch****

* **Enable S3 Event Notifications**:
* Go to the bucket where files are uploaded.
* Navigate to the **Properties** tab.
* Under **Event notifications**, configure a notification to trigger on file upload events (e.g., using the s3:ObjectCreated event).
* **Set Up CloudWatch Integration**:
* Create an AWS Lambda function to forward S3 event notifications to CloudWatch logs.
* Ensure the Lambda function has an IAM role with permissions to read from S3 and write to CloudWatch Logs.
* **Verify Logs**:
* Navigate to the **CloudWatch Logs** service.
* View the log streams for the Lambda function, which will contain details of uploaded files



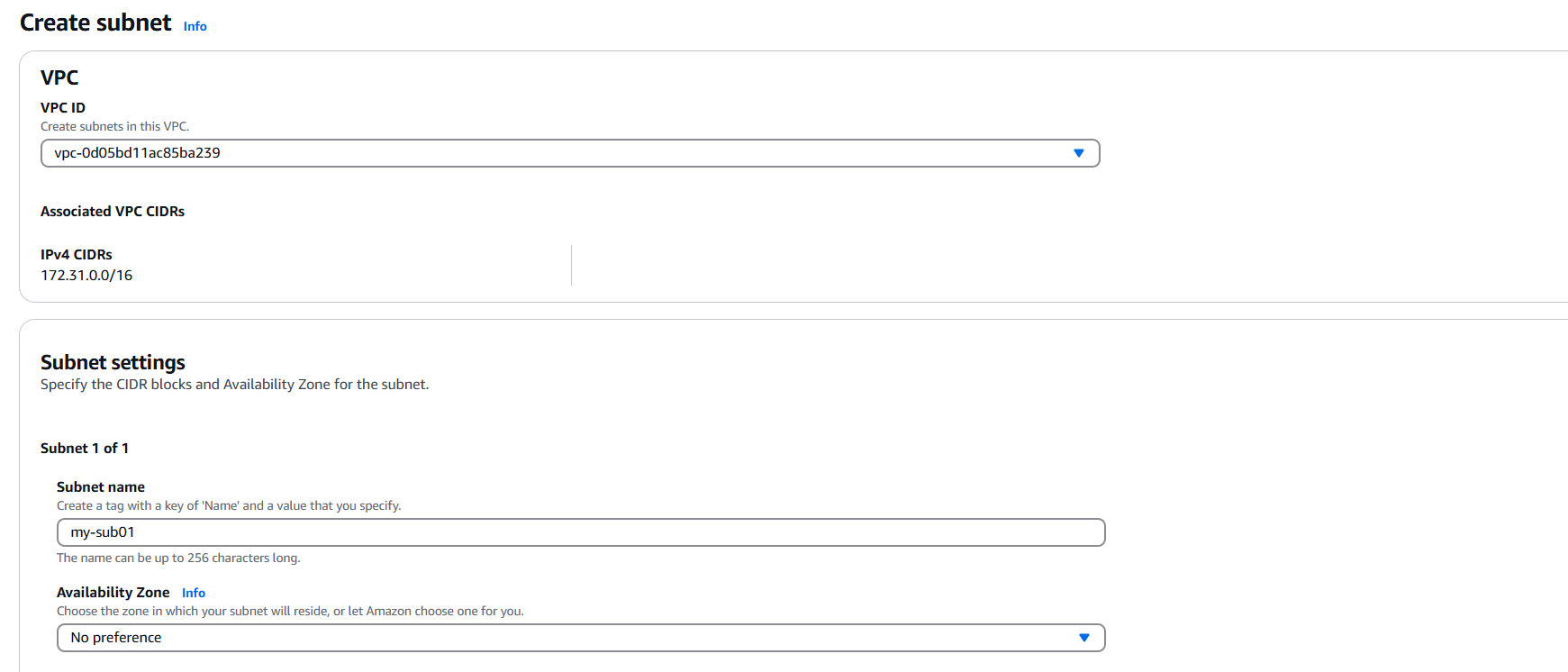


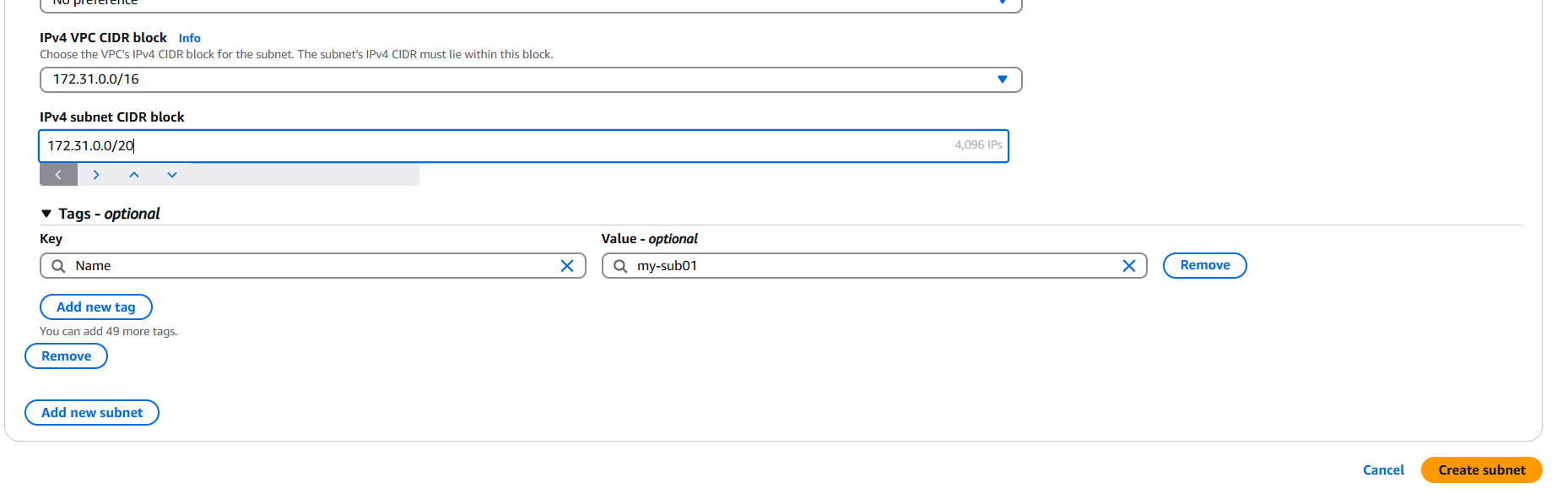


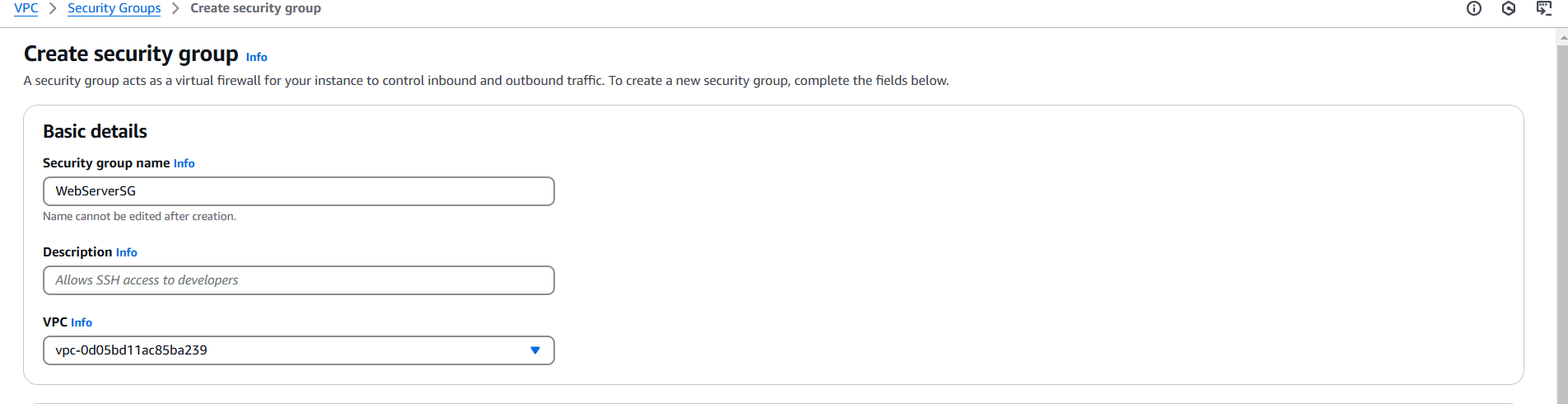


1. Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address.

In the search bar at the top, type **EC2** and select **EC2 Dashboard**. **Navigate to VPC Dashboard** Similarly, type **VPC** in the search bar and select **VPC Dashboard crete subnet** . **Create a Security Group** Allow **HTTP (port 80)** and **SSH (port 22)** for your EC2 instances.Configure necessary inbound and outbound rules. **Set up a Key Pair**: Go to **EC2 Key Pairs** and create a new key pair or use an existing one for SSH access to the EC2 instances.  
  
****Launch 2 Instances****: Navigate to ****EC2 > Instances**** and click ****Launch Instances****.Choose an Amazon Linux or Ubuntu AMI.Choose instance type (e.g., t2.micro for free tier). Configure the instances in the same ****VPC**** and ****Subnet****.

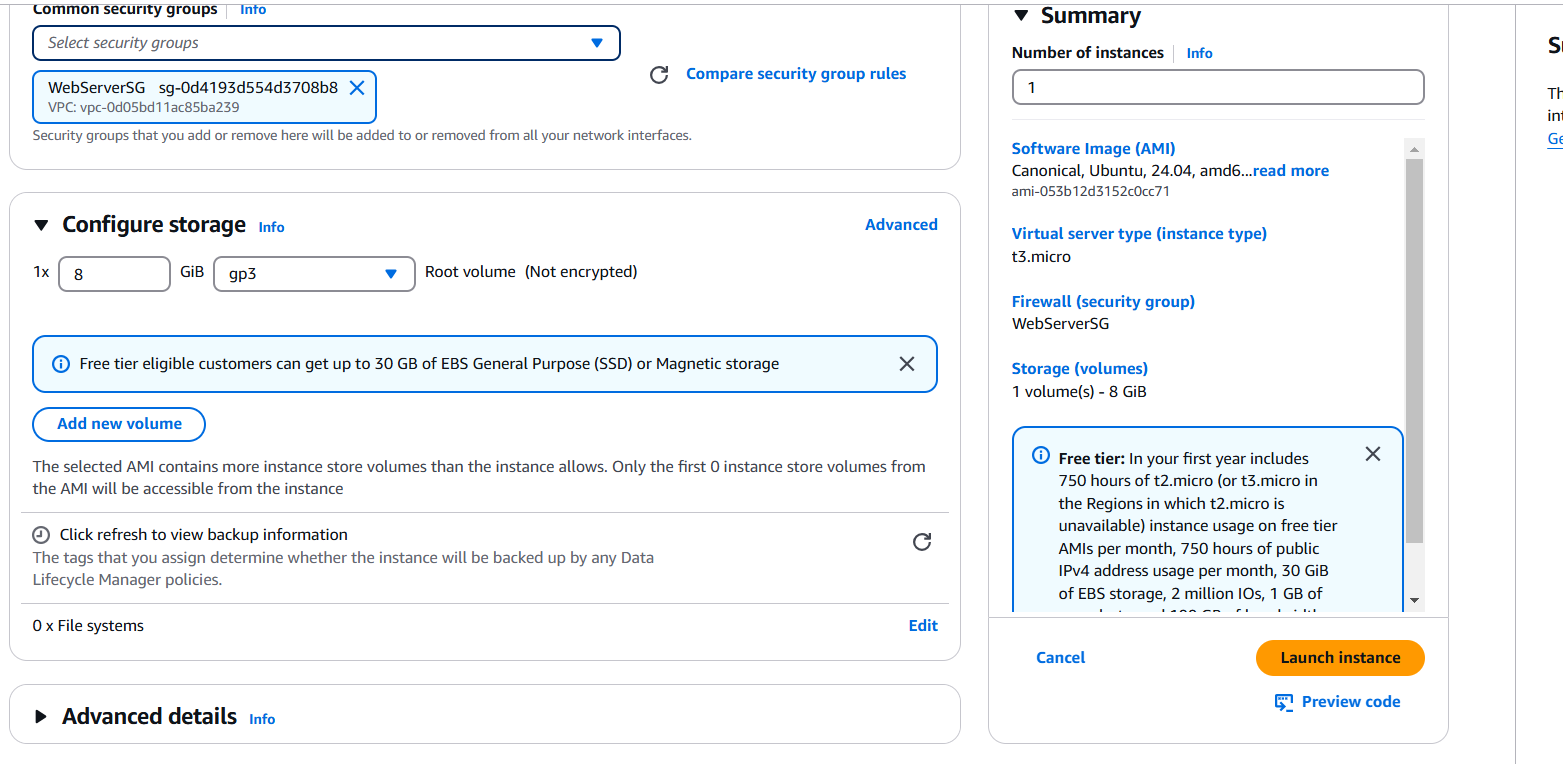


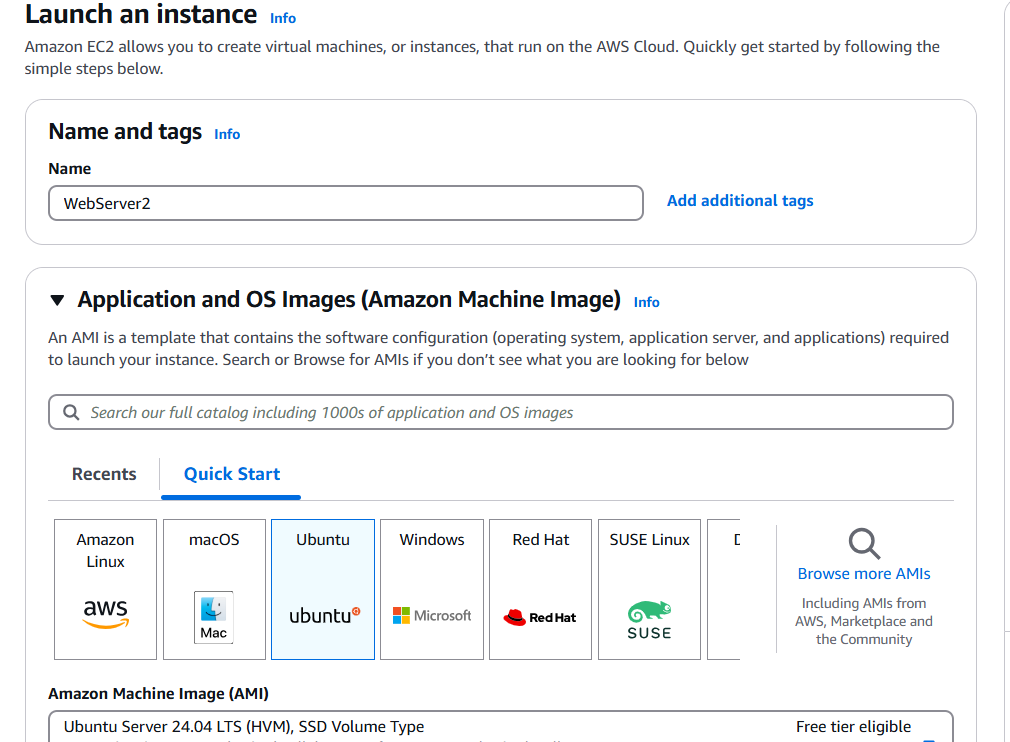


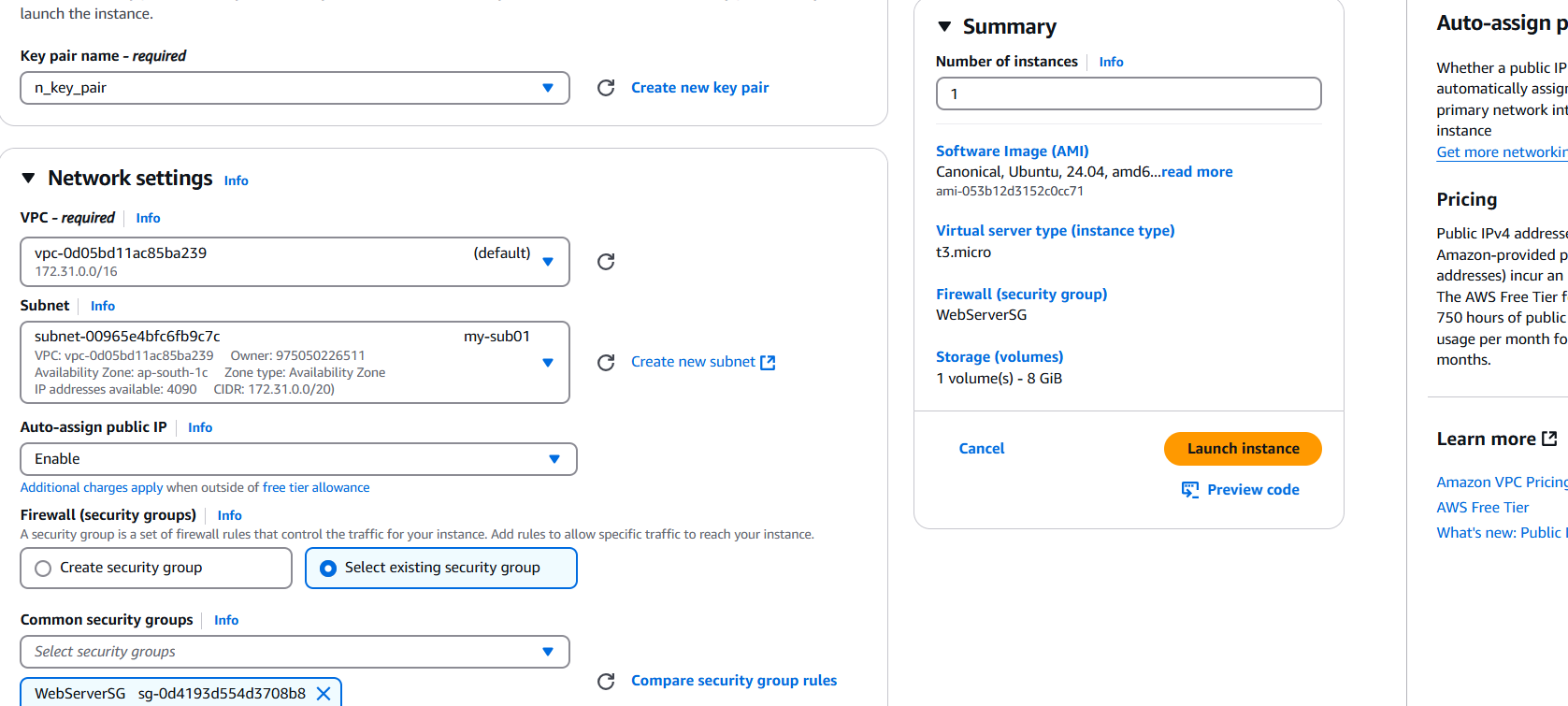


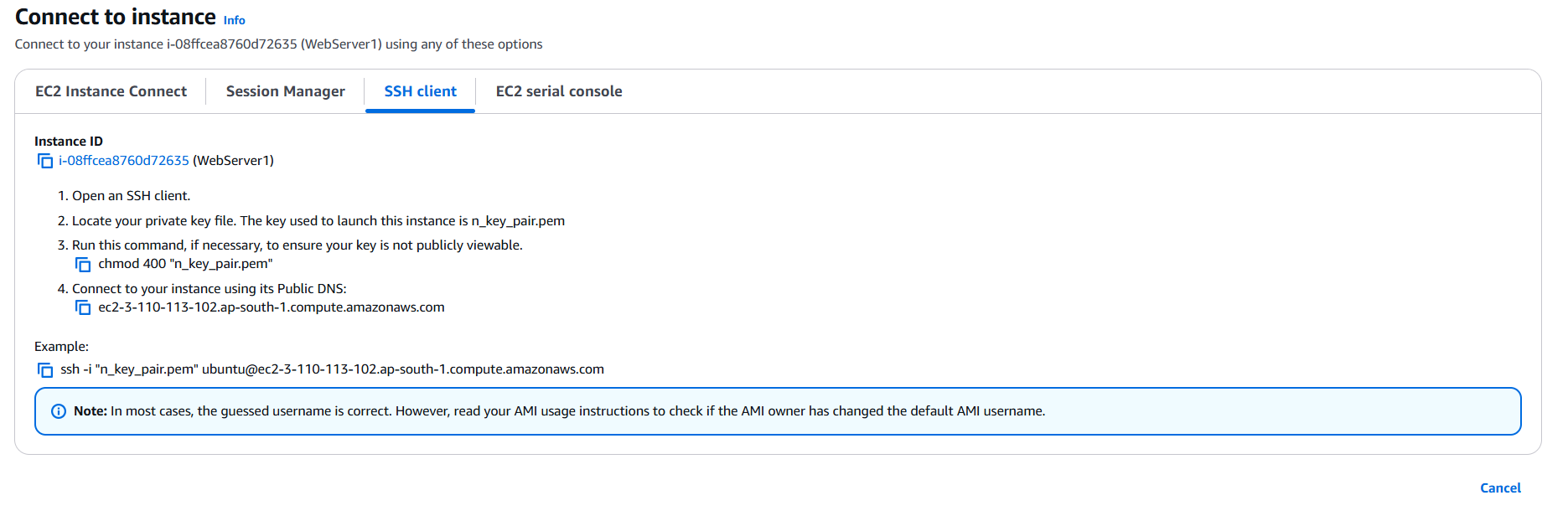


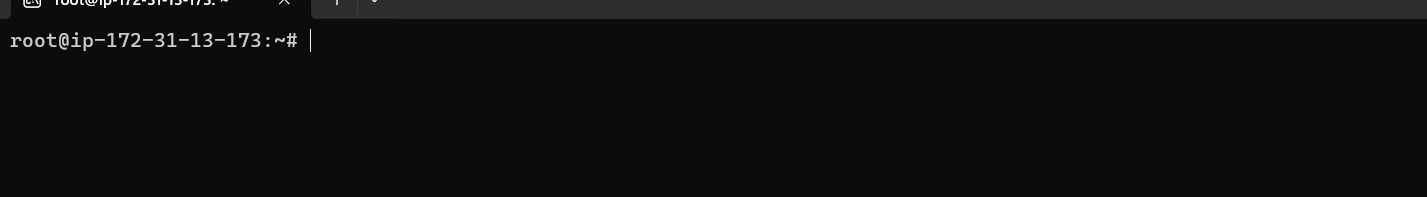
### 









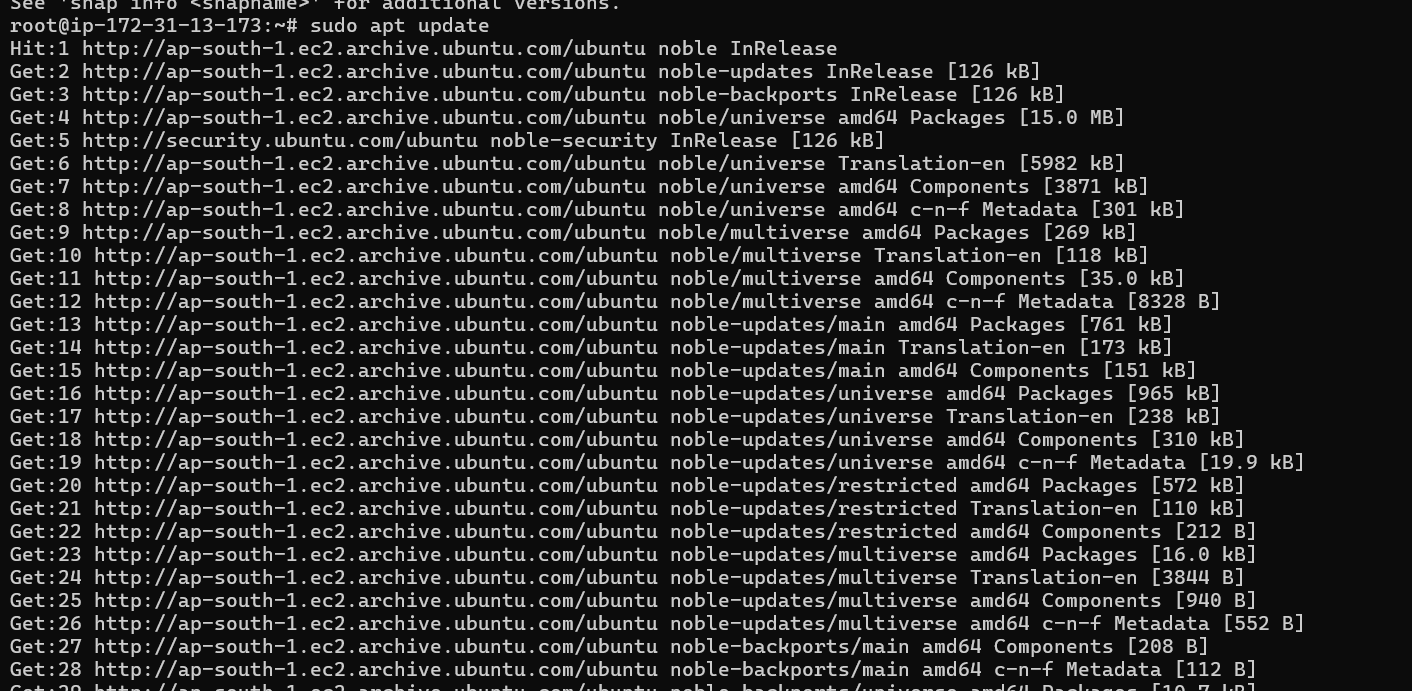


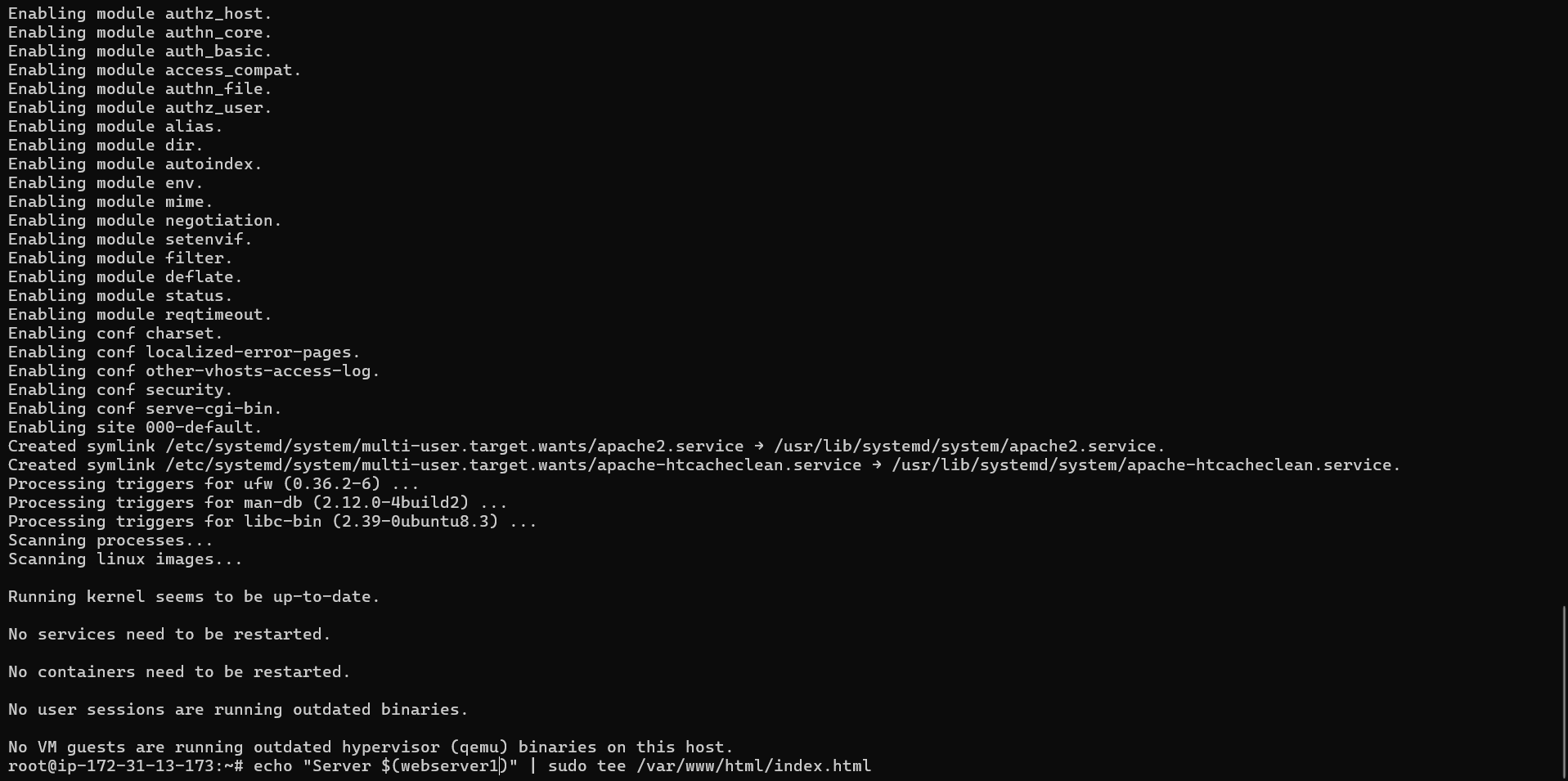
Install and start a web server : Install Apache Web Server , Configure the Web Server , Start the Apache service , Enable the service to start on boot Repeat for the Second Instance  
sudo yum update -y

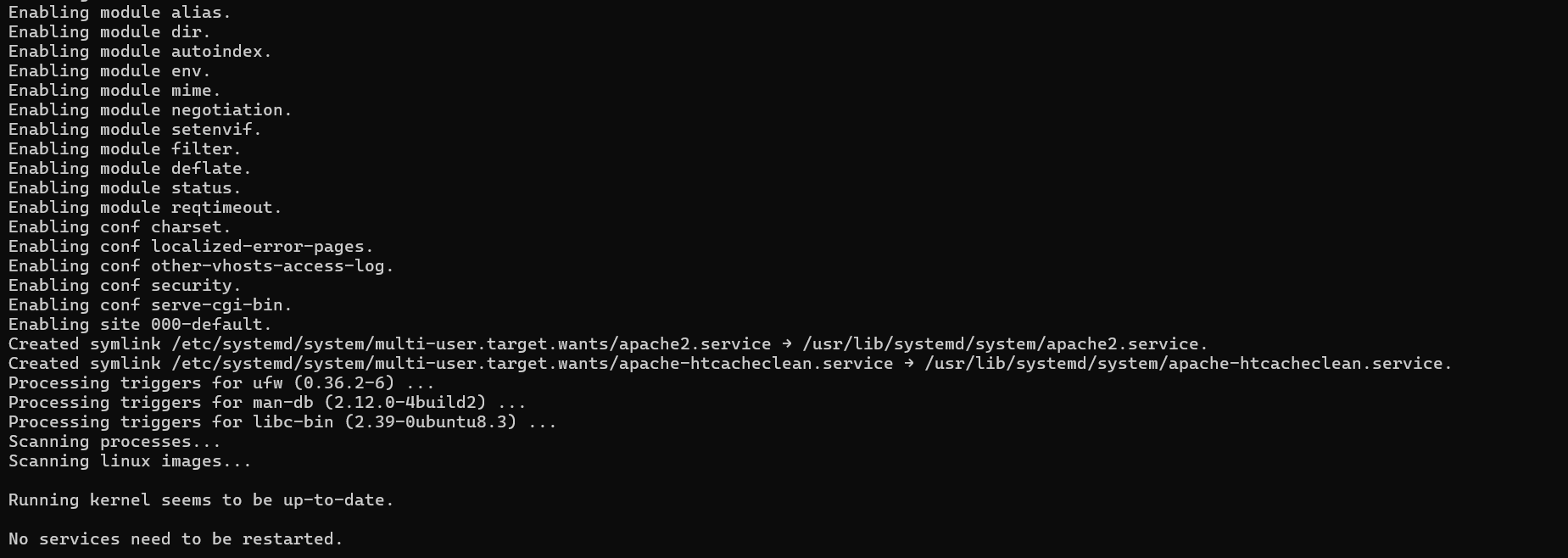
sudo yum install httpd -yecho "Server $(hostname)" | sudo tee /var/www/html/index.html

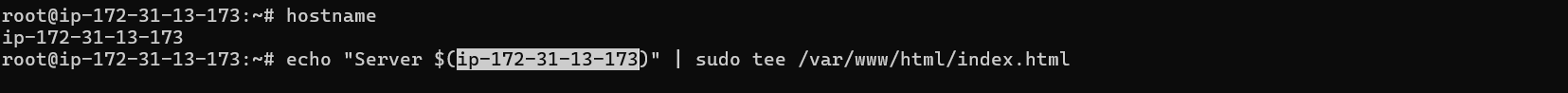
sudo systemctl start httpd

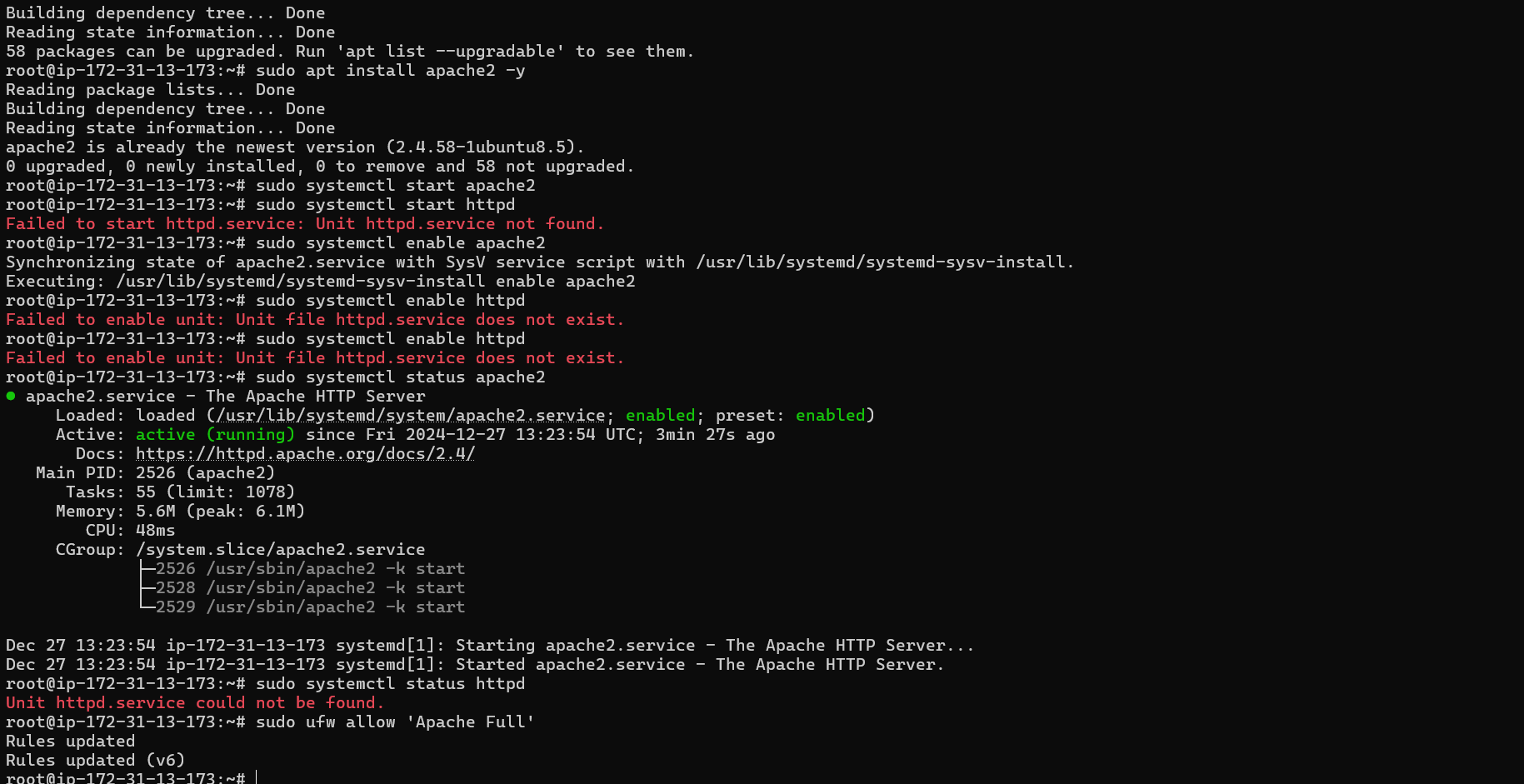
sudo systemctl enable httpd







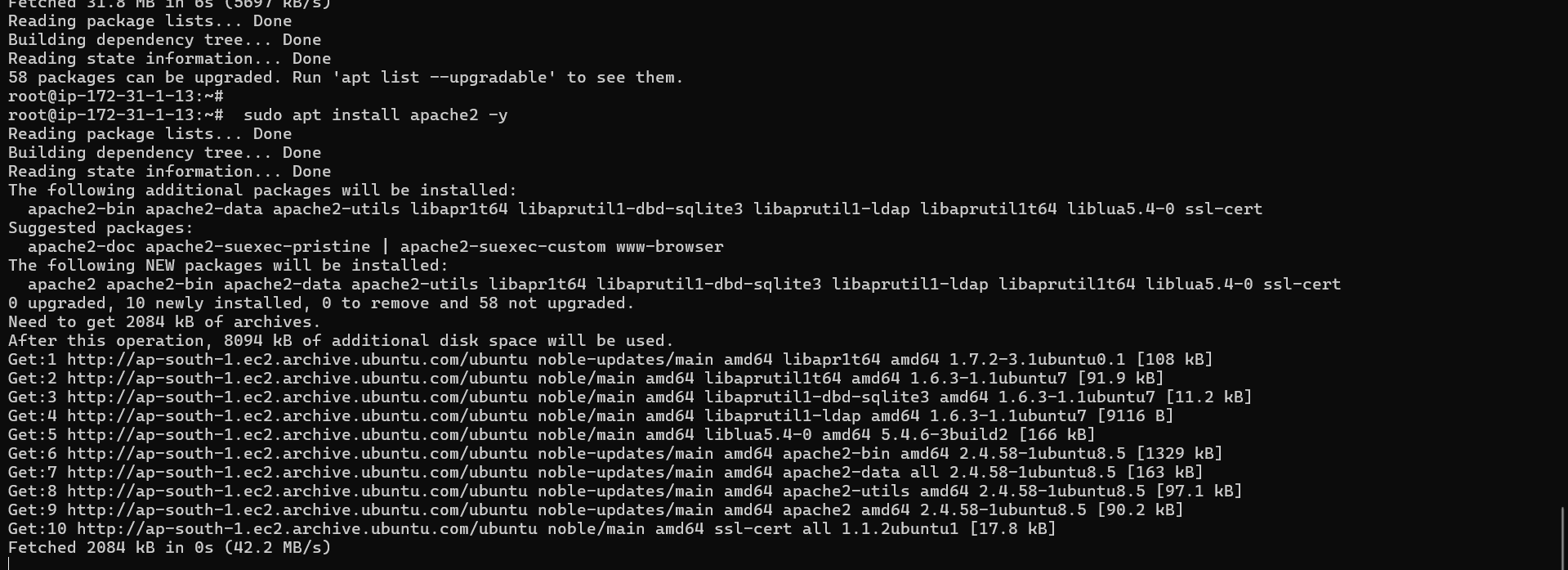


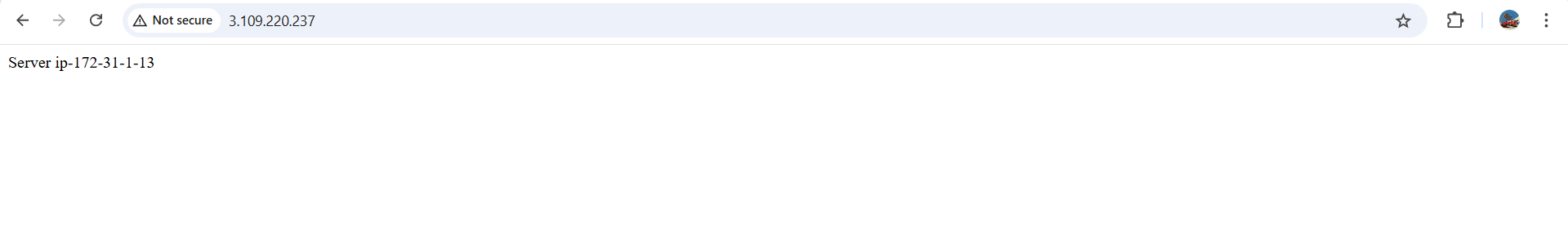




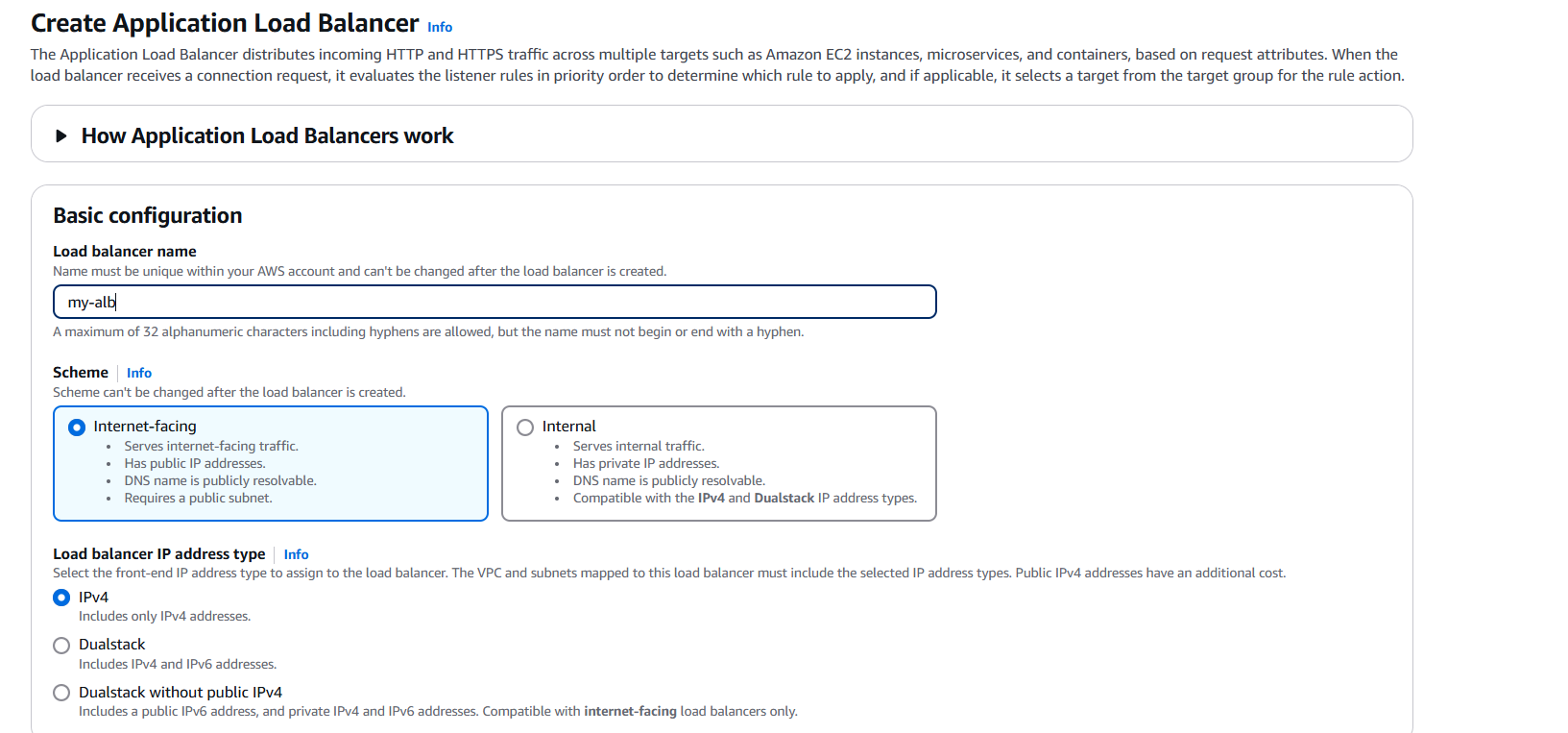
Instance 2

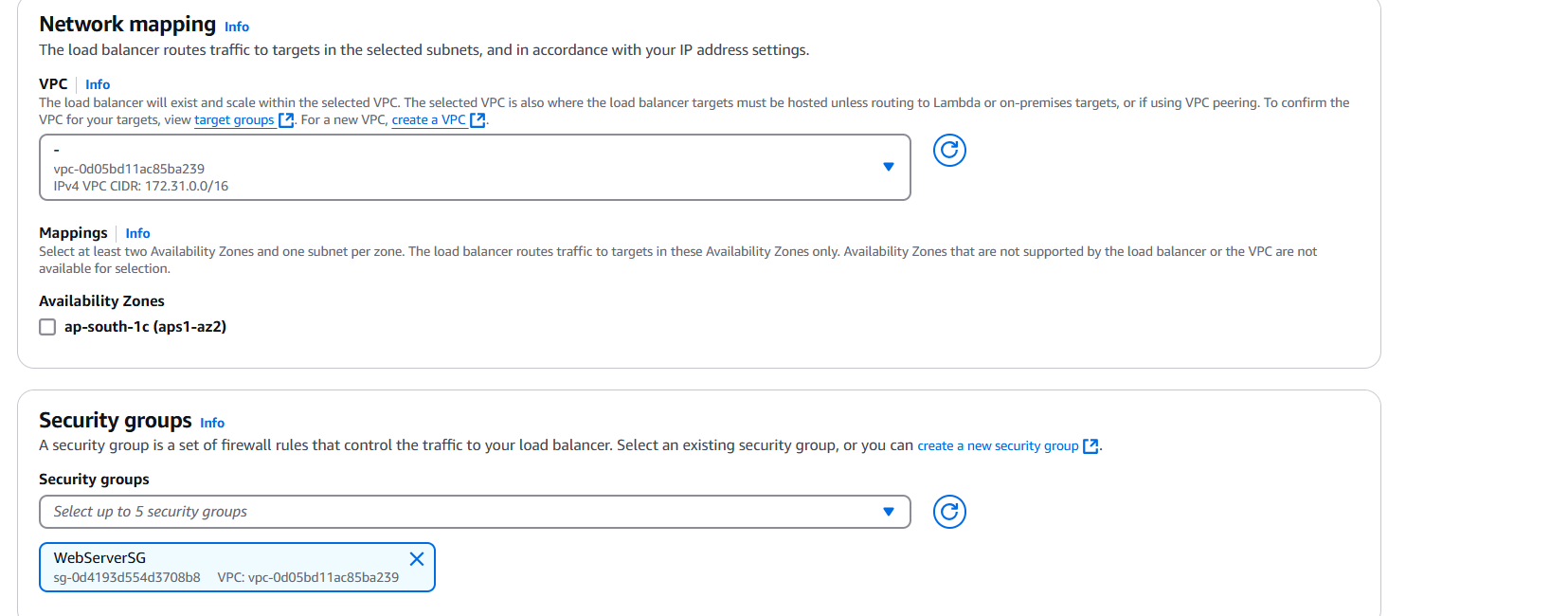


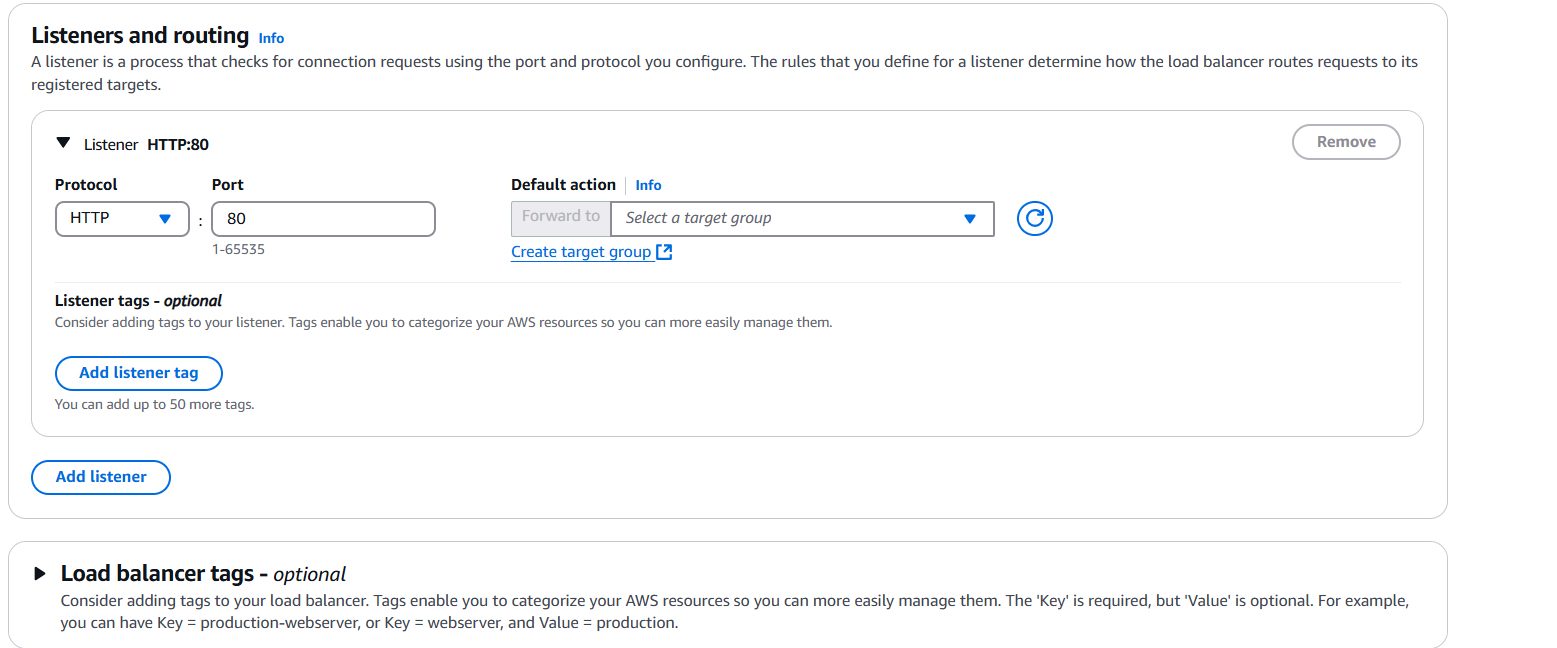




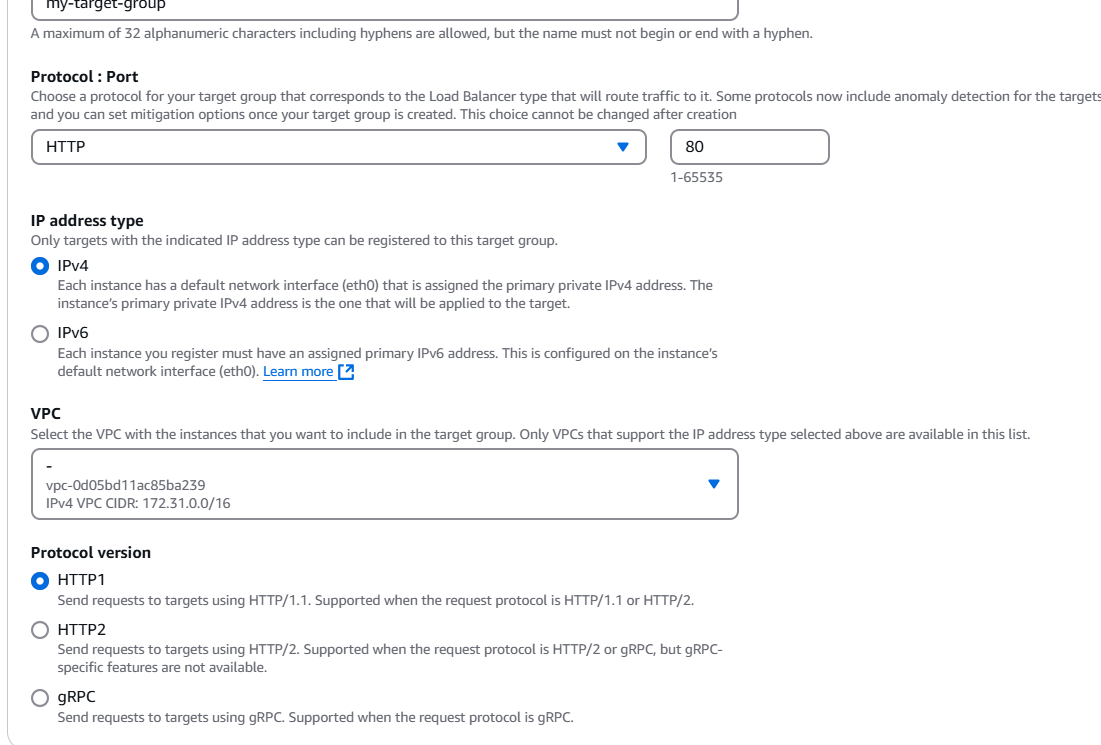
### ****Create an Application Load Balancer (ALB)Navigate to the Load Balancer Section****:Go to ****EC2 > Load Balancers**** and click ****Create Load Balancer****.Choose ****Application Load Balancer****.****Configure the Load Balancer****:Set a name (e.g., My-ALB).Choose ****Internet-facing**** for the scheme.Select the same ****VPC**** and subnets where the instances are deployed.****Configure the Security Group****:Assign a security group to allow HTTP (port 80).****Create a Target Group****:Select ****Instances**** as the target type.Register your two EC2 instances to this target group.****Assign Target Group to the Load Balancer****:During ALB creation, assign the newly created target group.****Finish and Verify****:Complete the ALB setup and test by accessing the ALB's DNS name (available in the Load Balancer details).

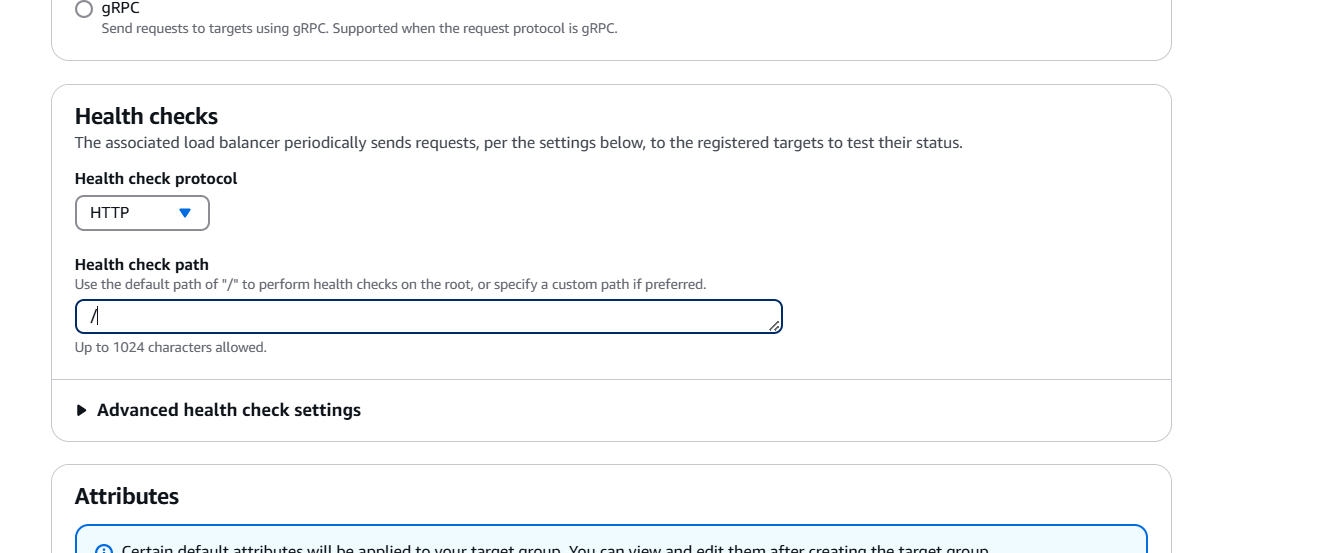


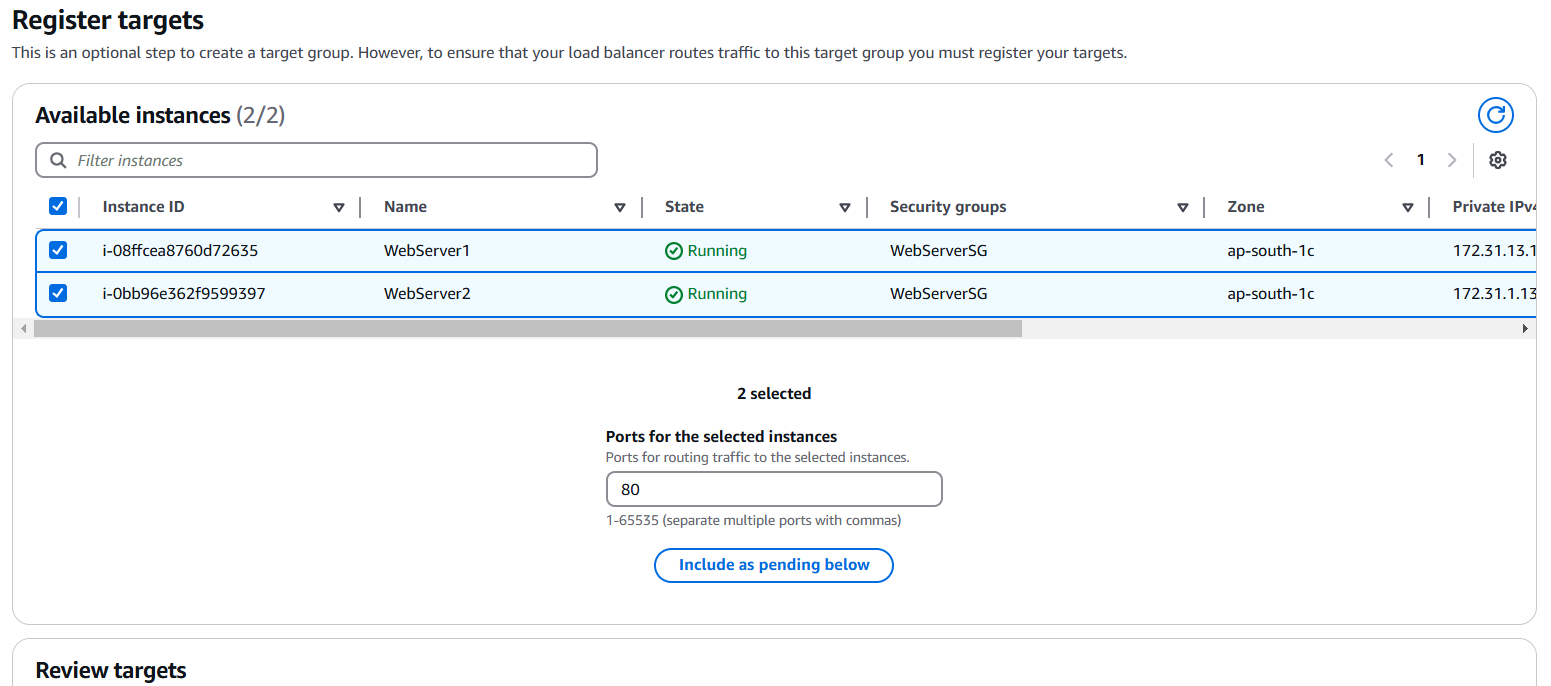


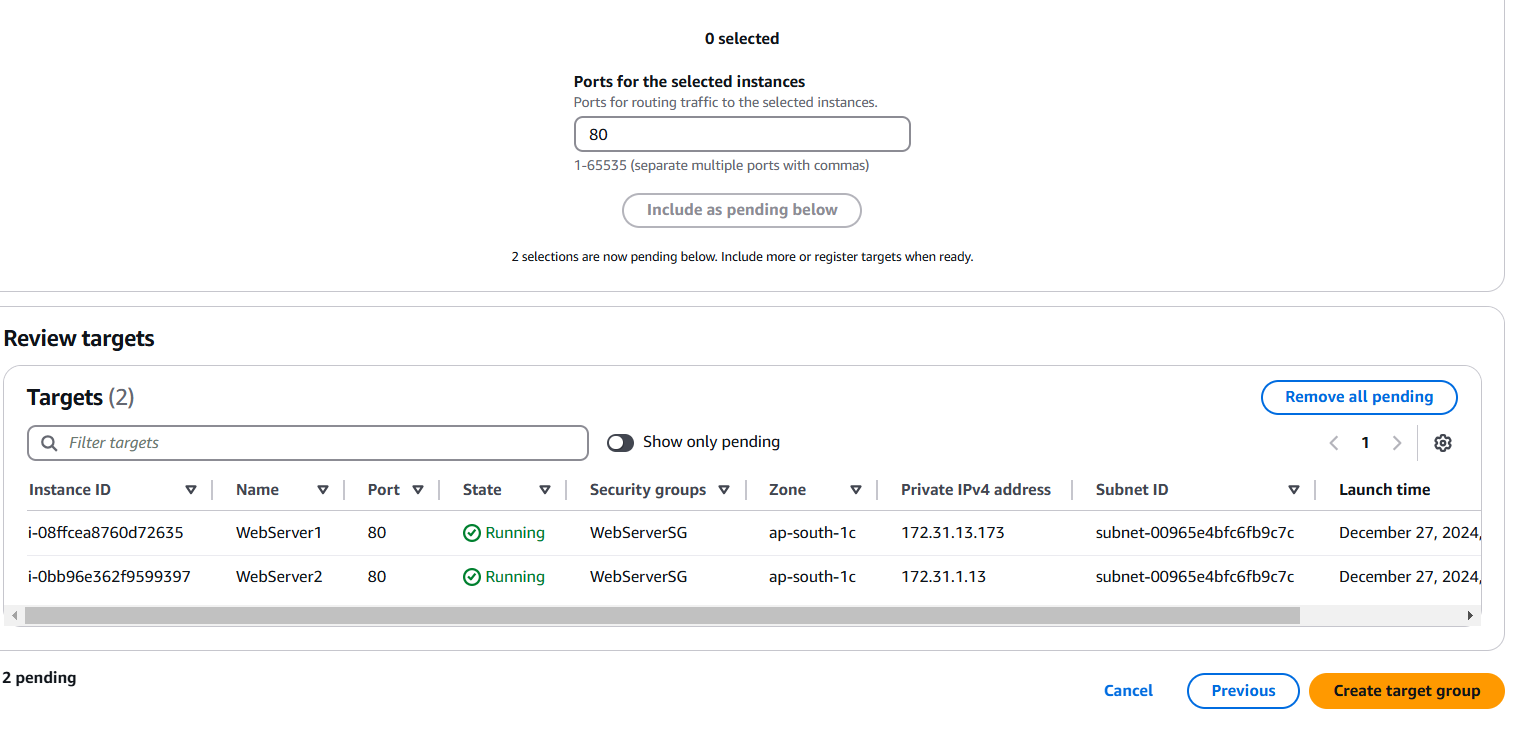


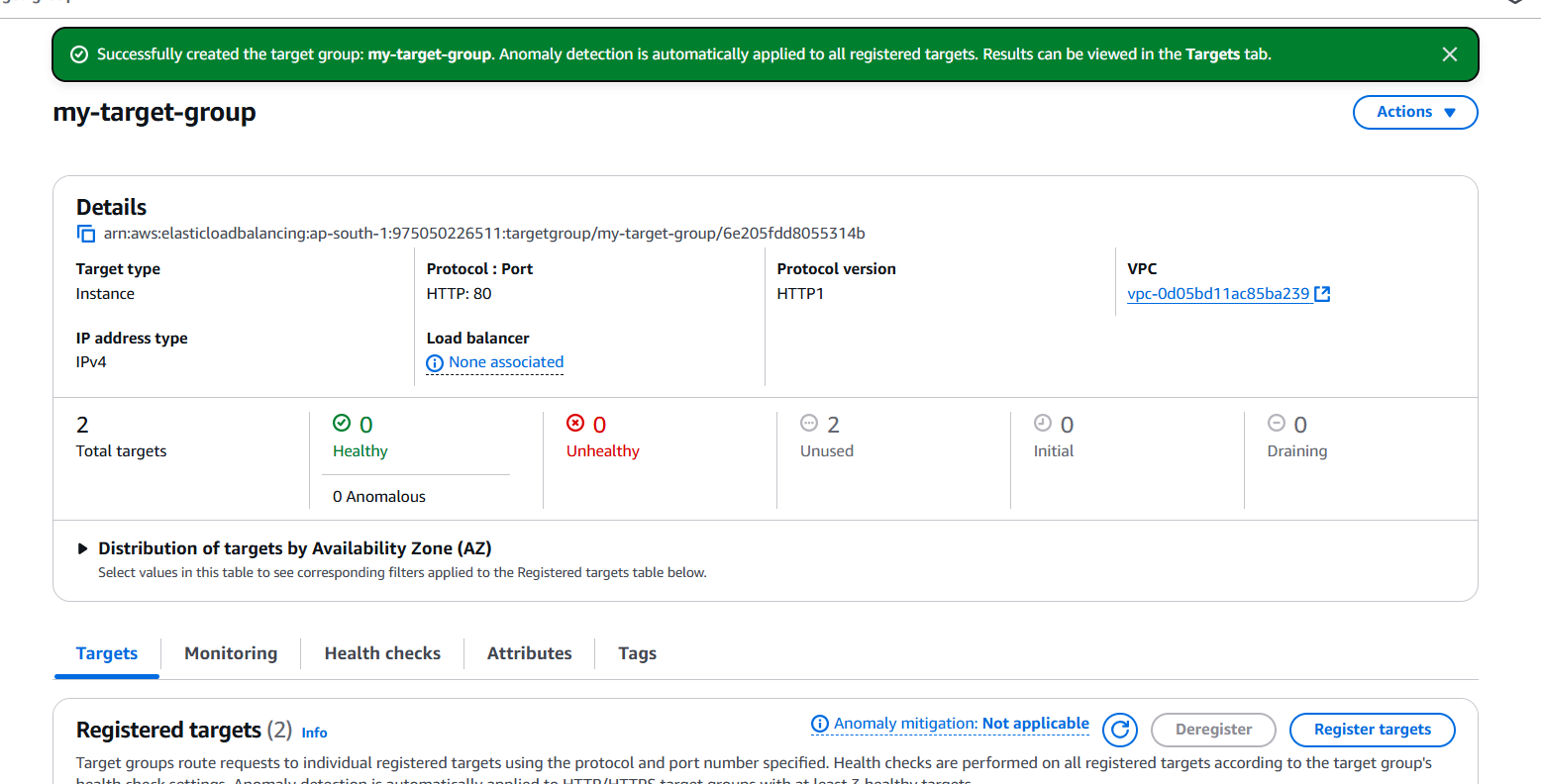


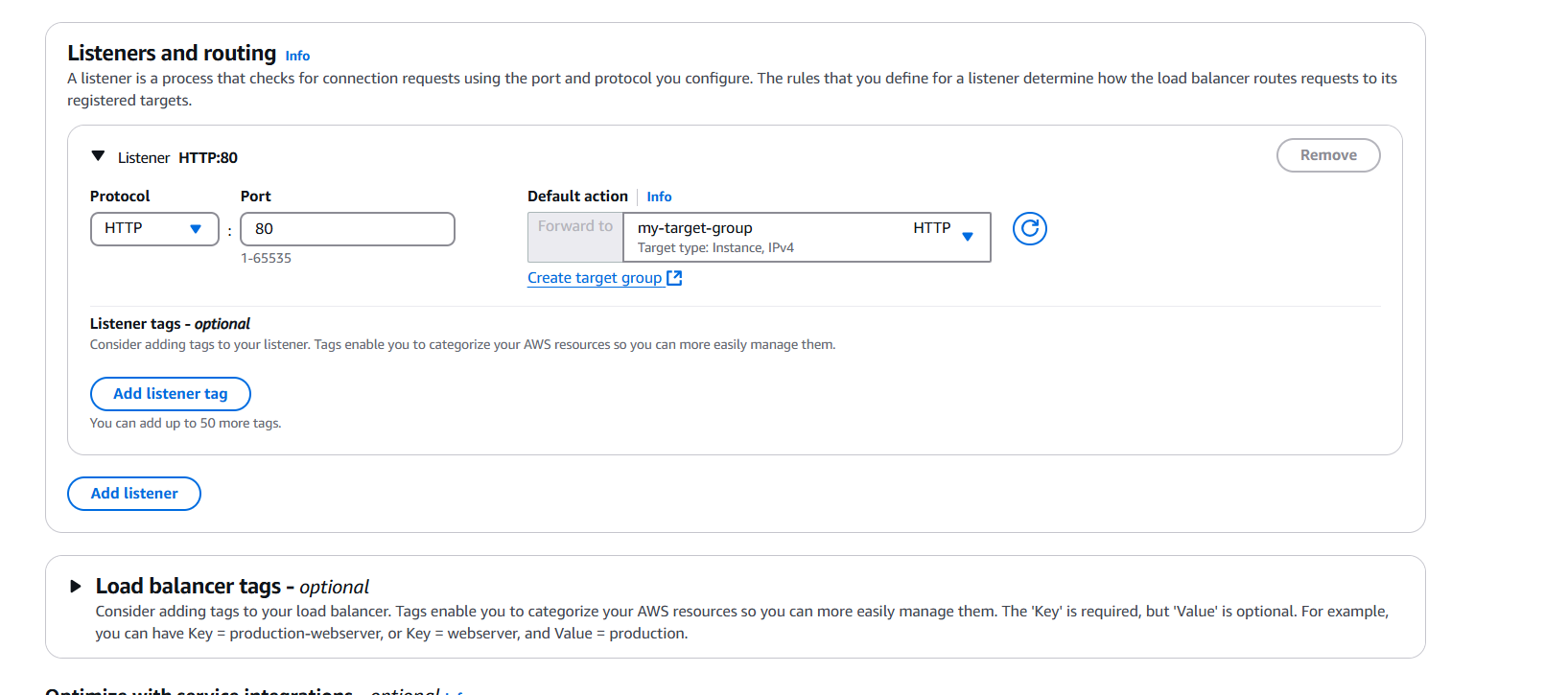


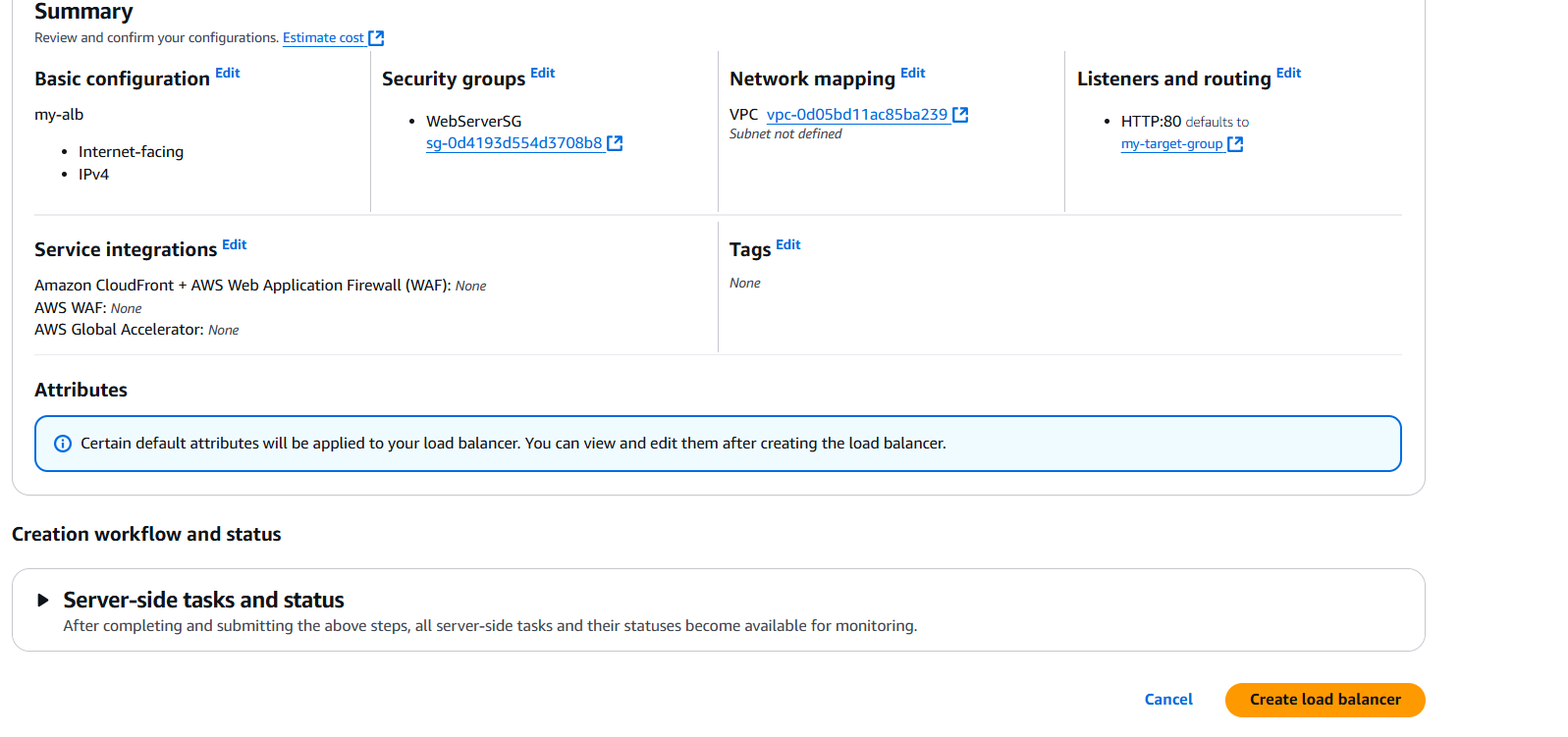


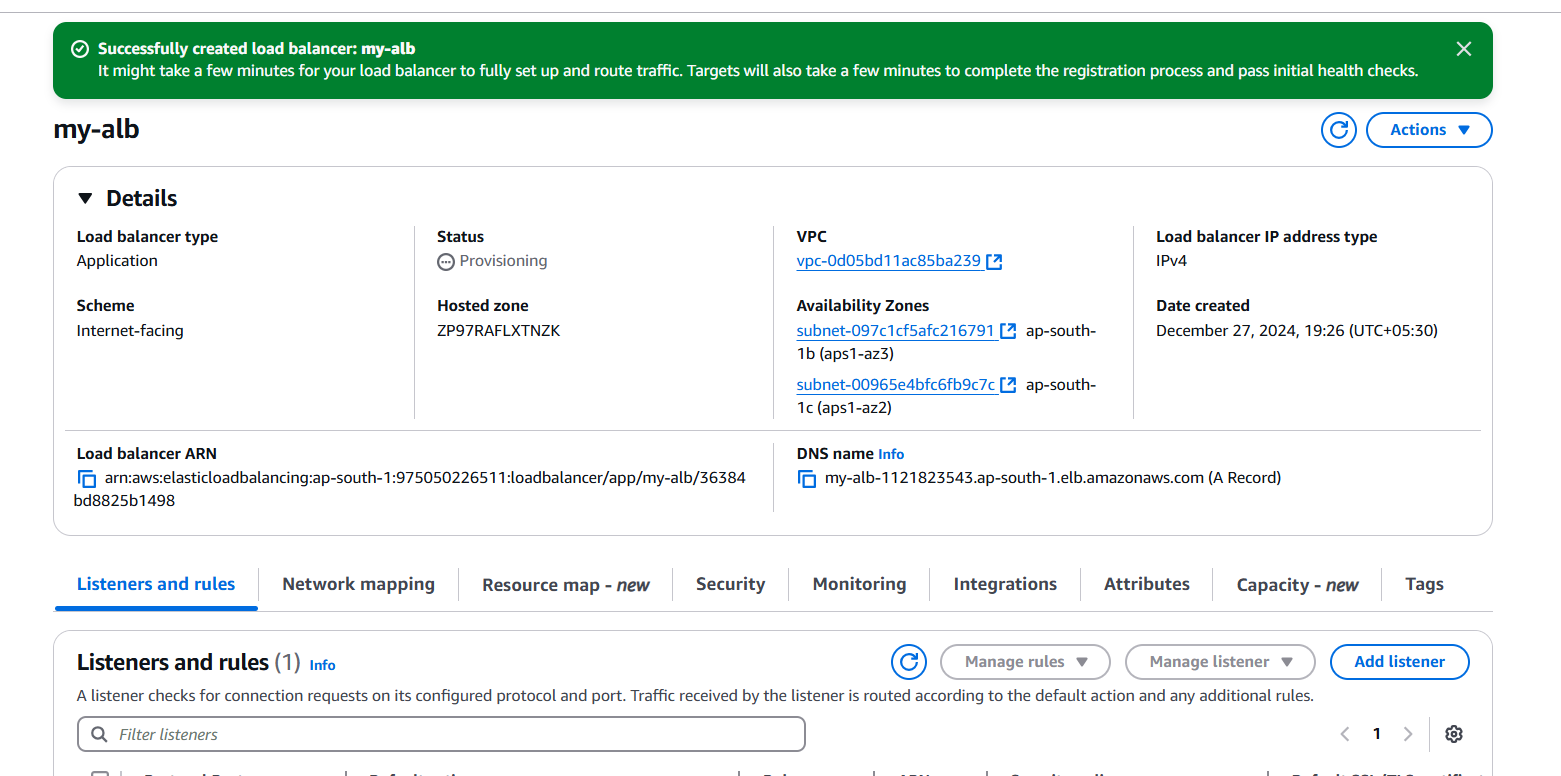












**Testing**:

Test the outgoing IP using an external service (e.g., curl ifconfig.me). Verify traffic routes via the ALB.

