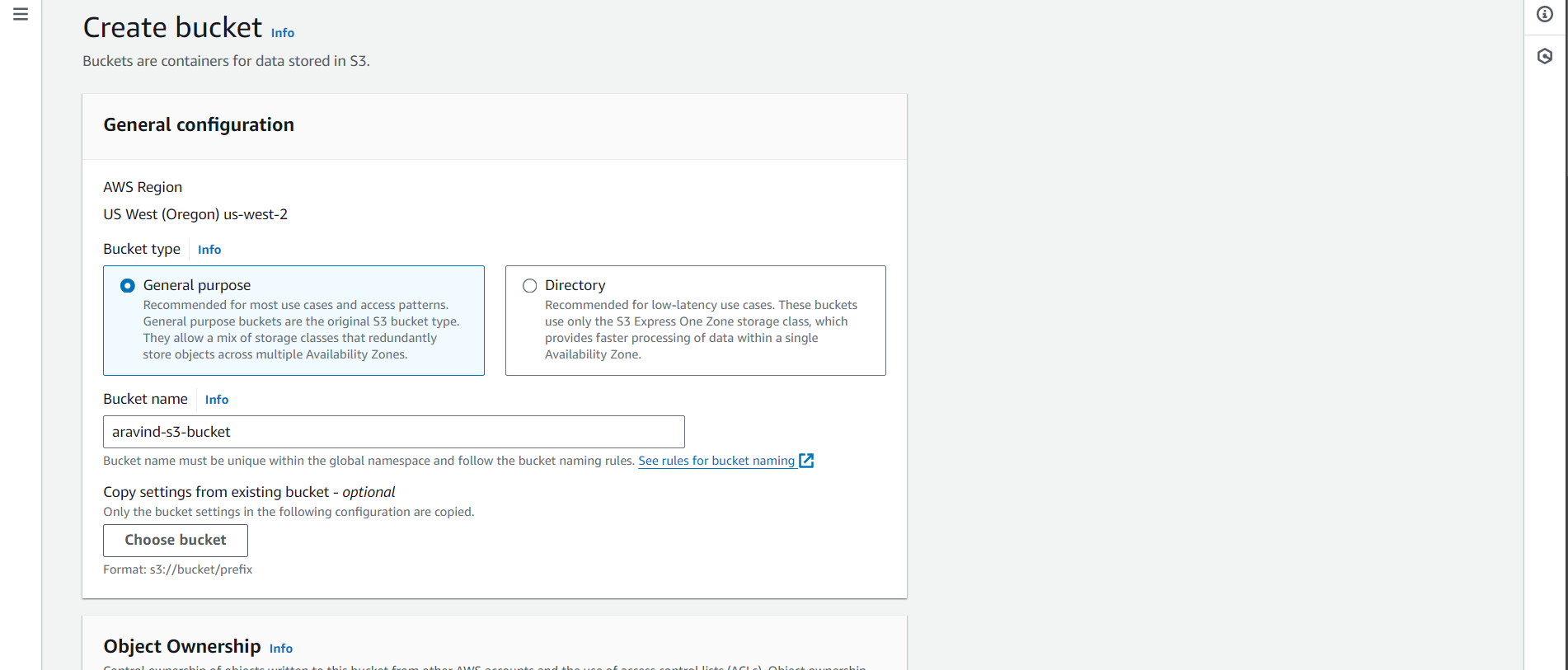
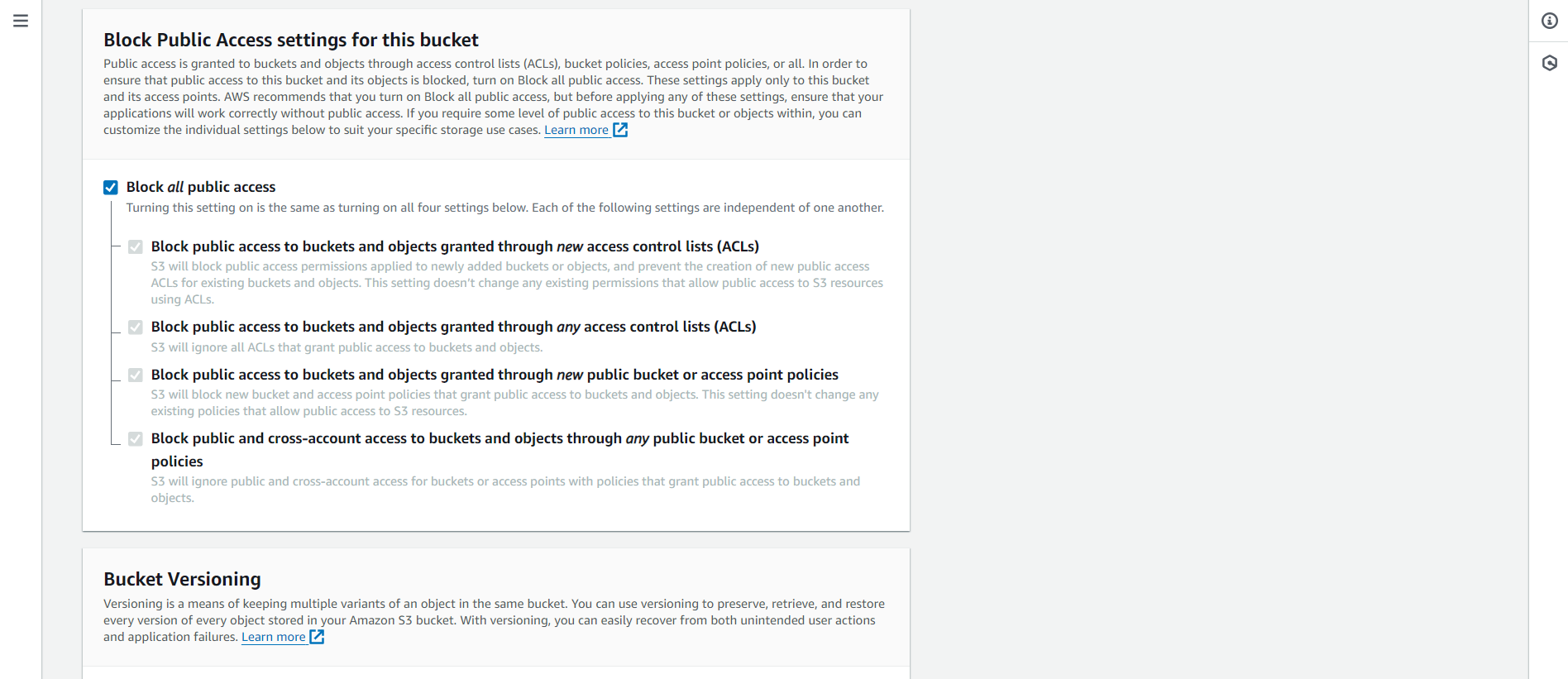
**AWS Task 3**

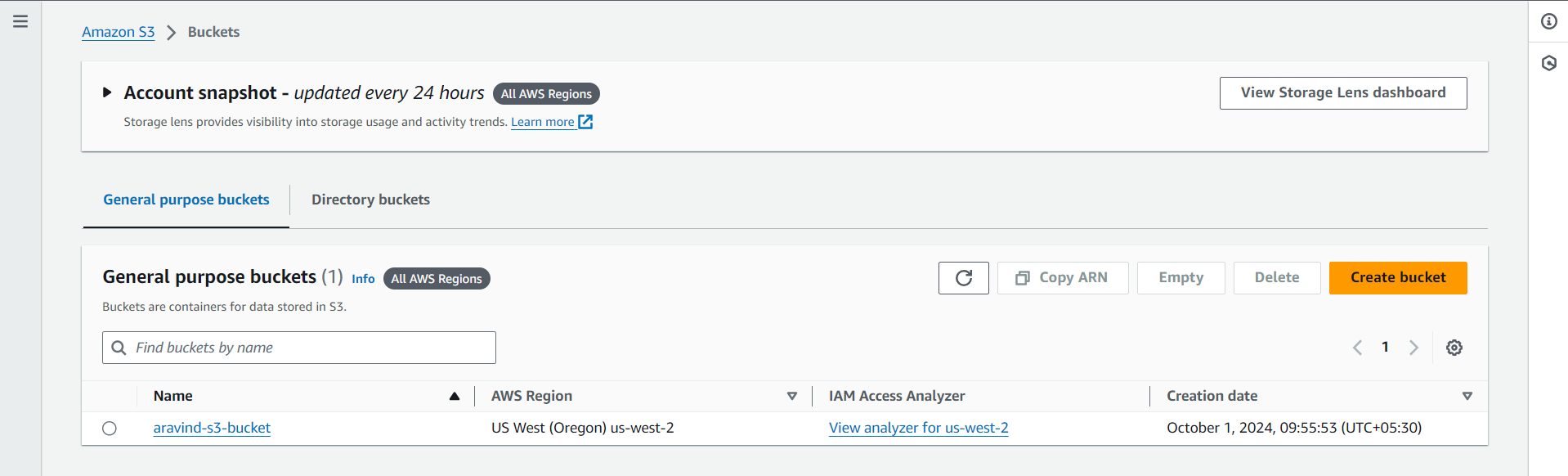
**1. Create a S3 bucket, with no public access and upload files to the bucket & view the logs using CloudWatch for the uploaded files.**

🡪Create a S3 Bucket in AWS with No public access

S3 🡪 Buckets 🡪 Create Bucket 🡪 Enter Bucket Name 🡪 Block ALL public access (Default) 🡪 Create Bucket

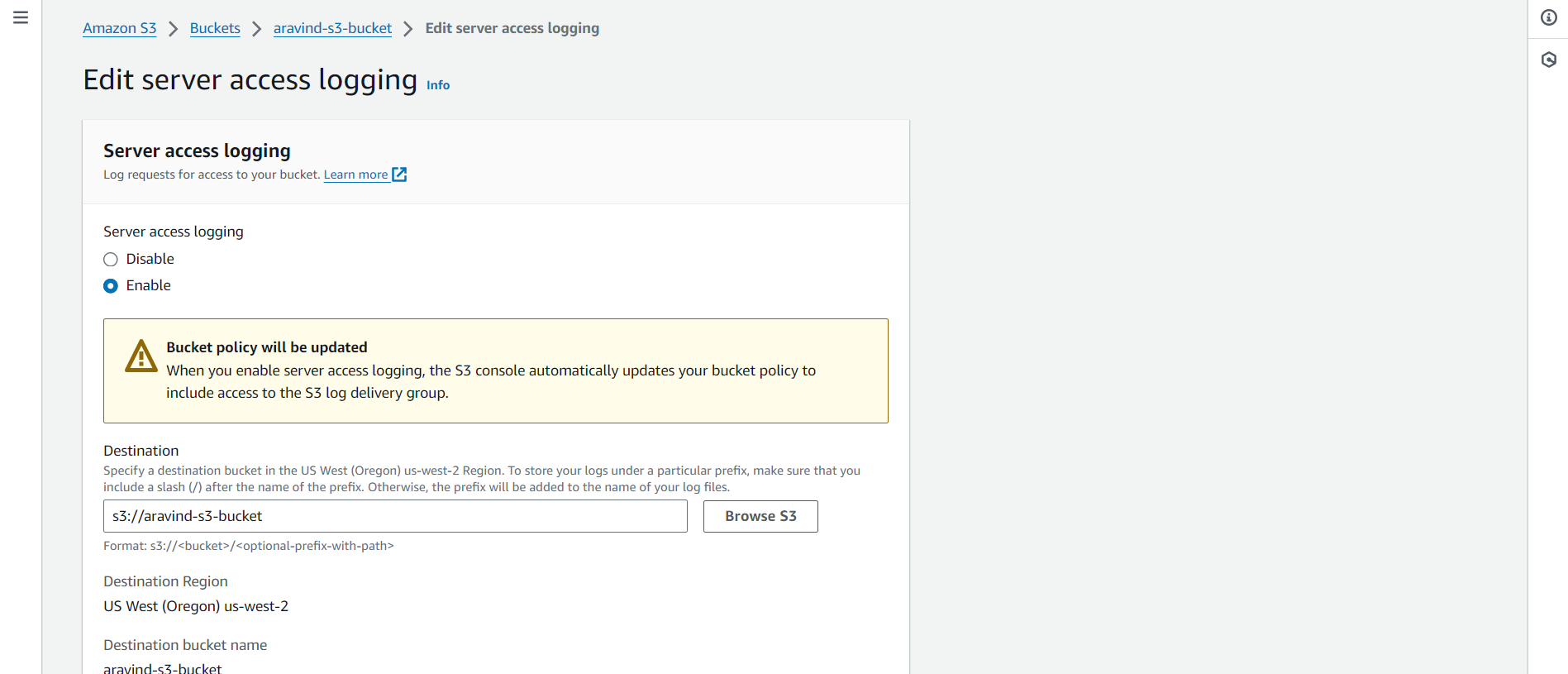


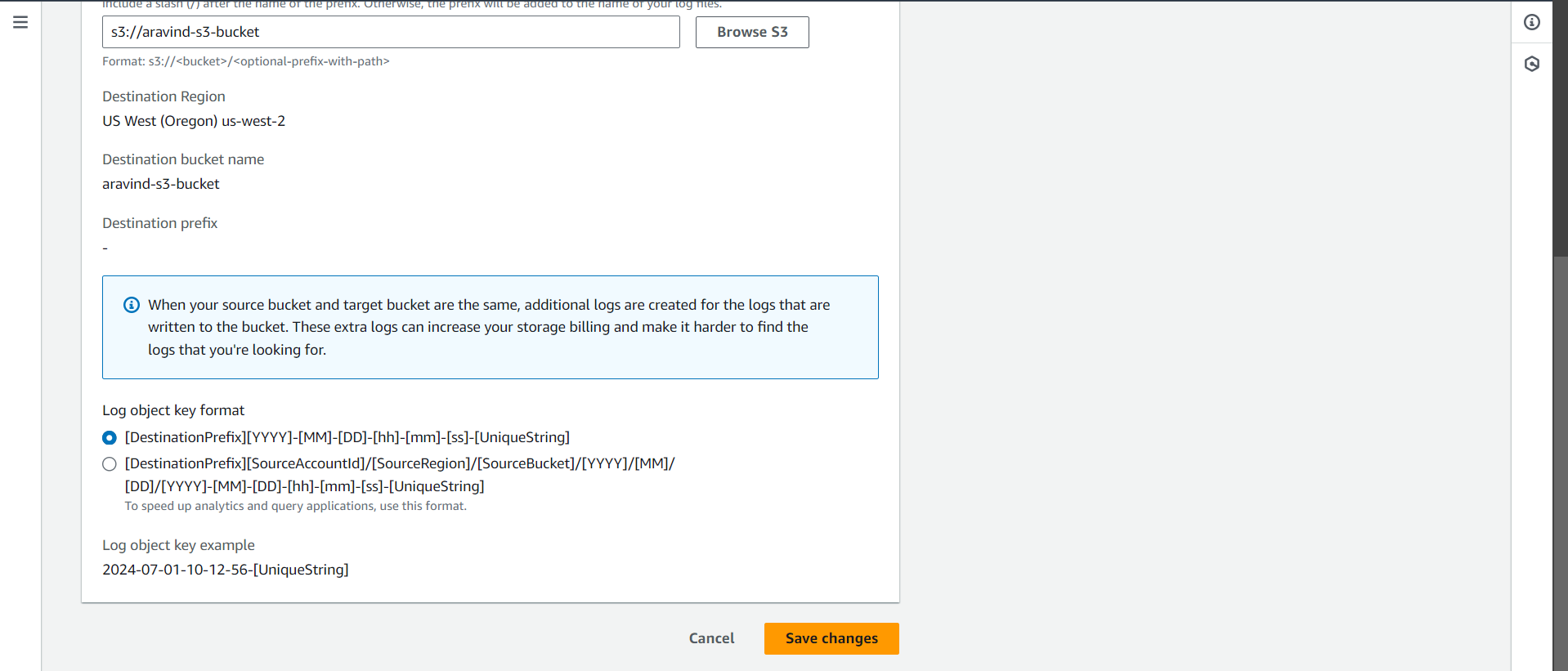




🡪Enable Server access Logging

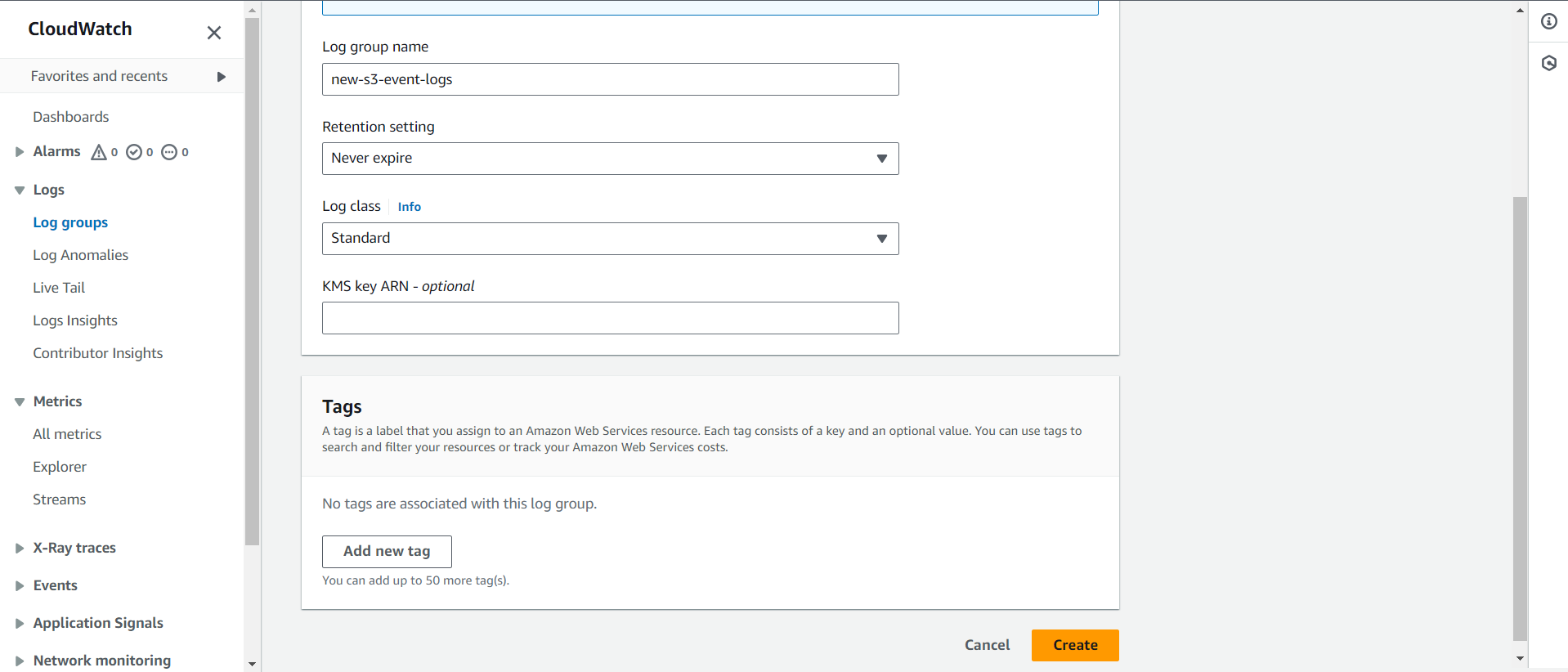
Select S3 bucket 🡪 Properties 🡪 Enable server access logging 🡪 select S3 bucket for destination 🡪 save changes

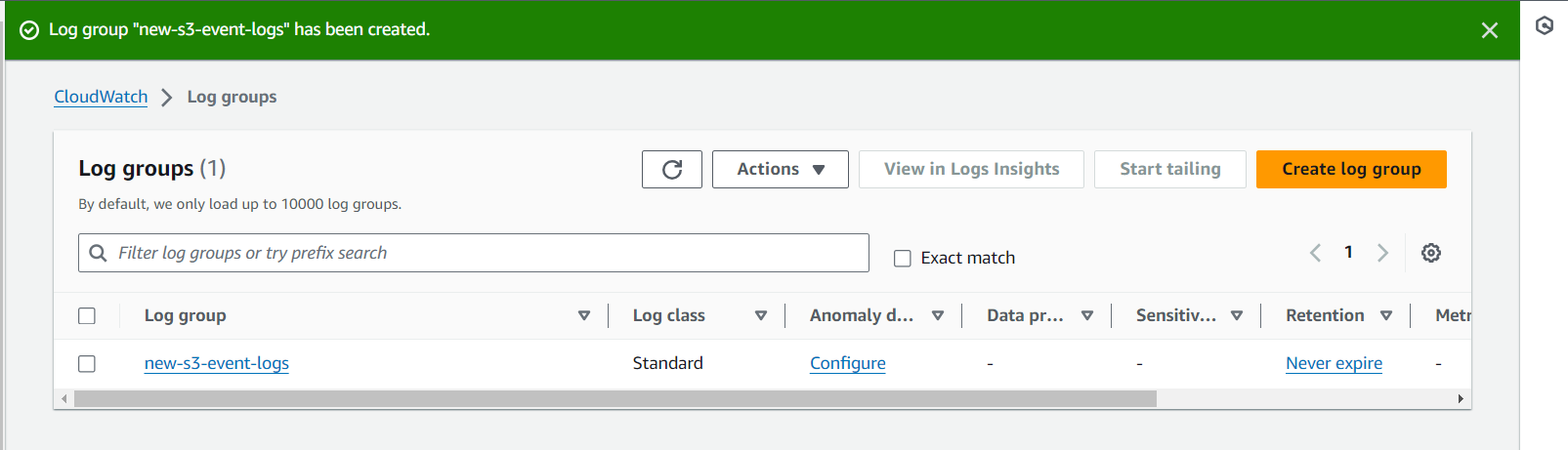




🡪Create CloudWatch Log Group

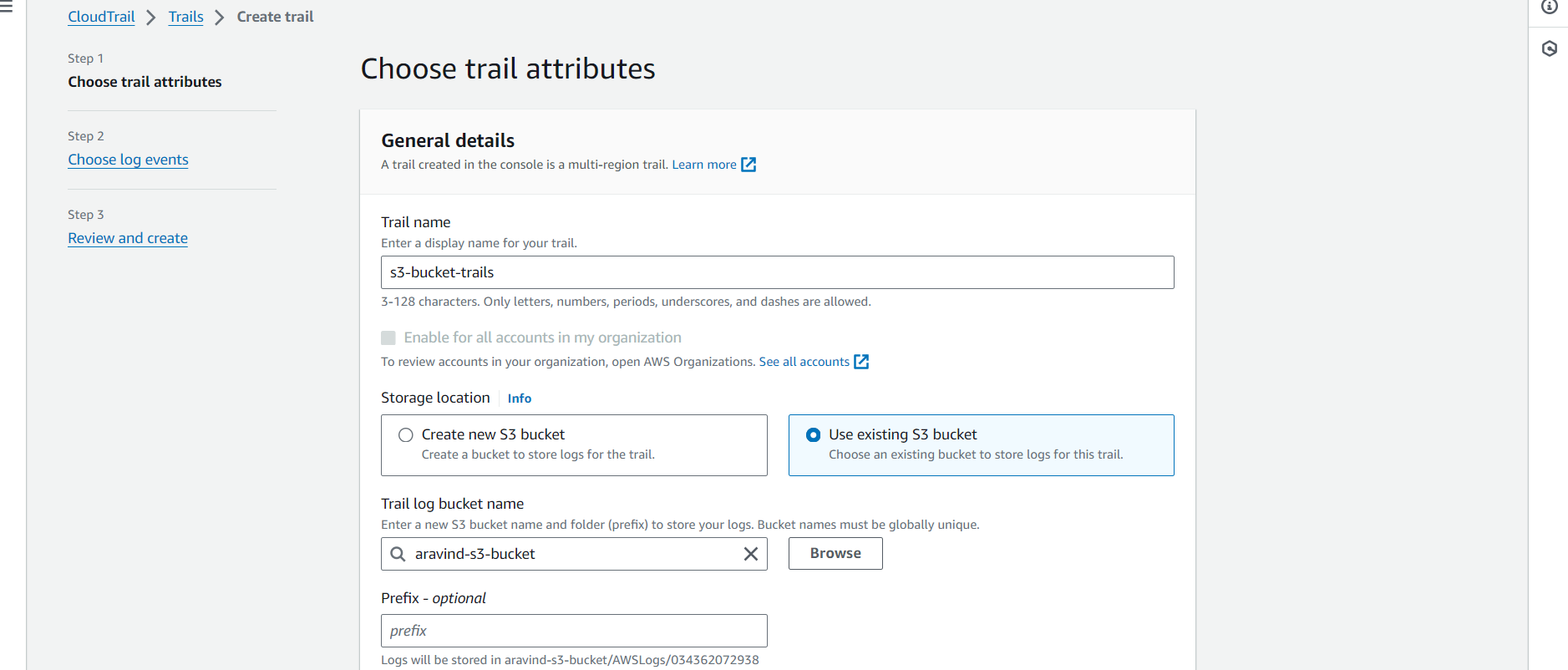
CloudWatch 🡪 Log Group 🡪 Create Log Group 🡪 enter name 🡪 create

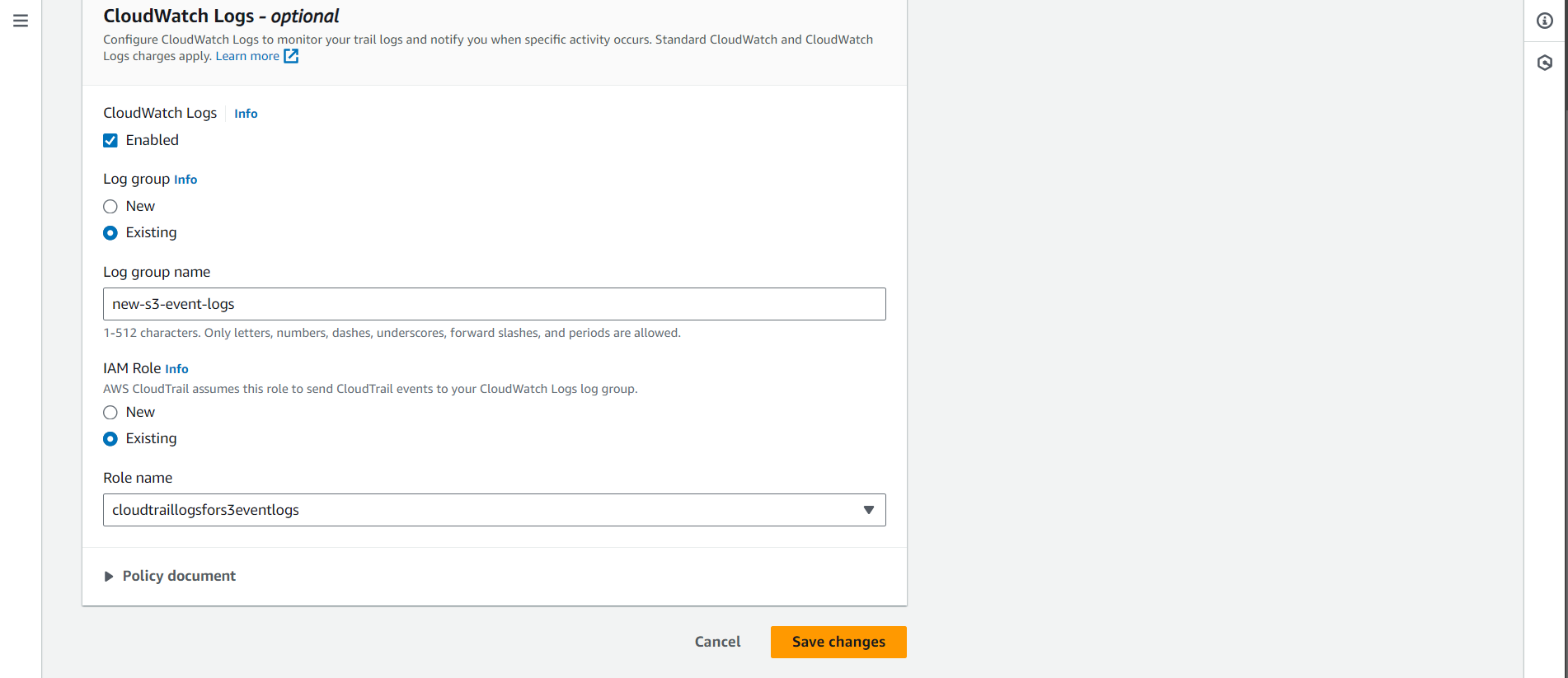


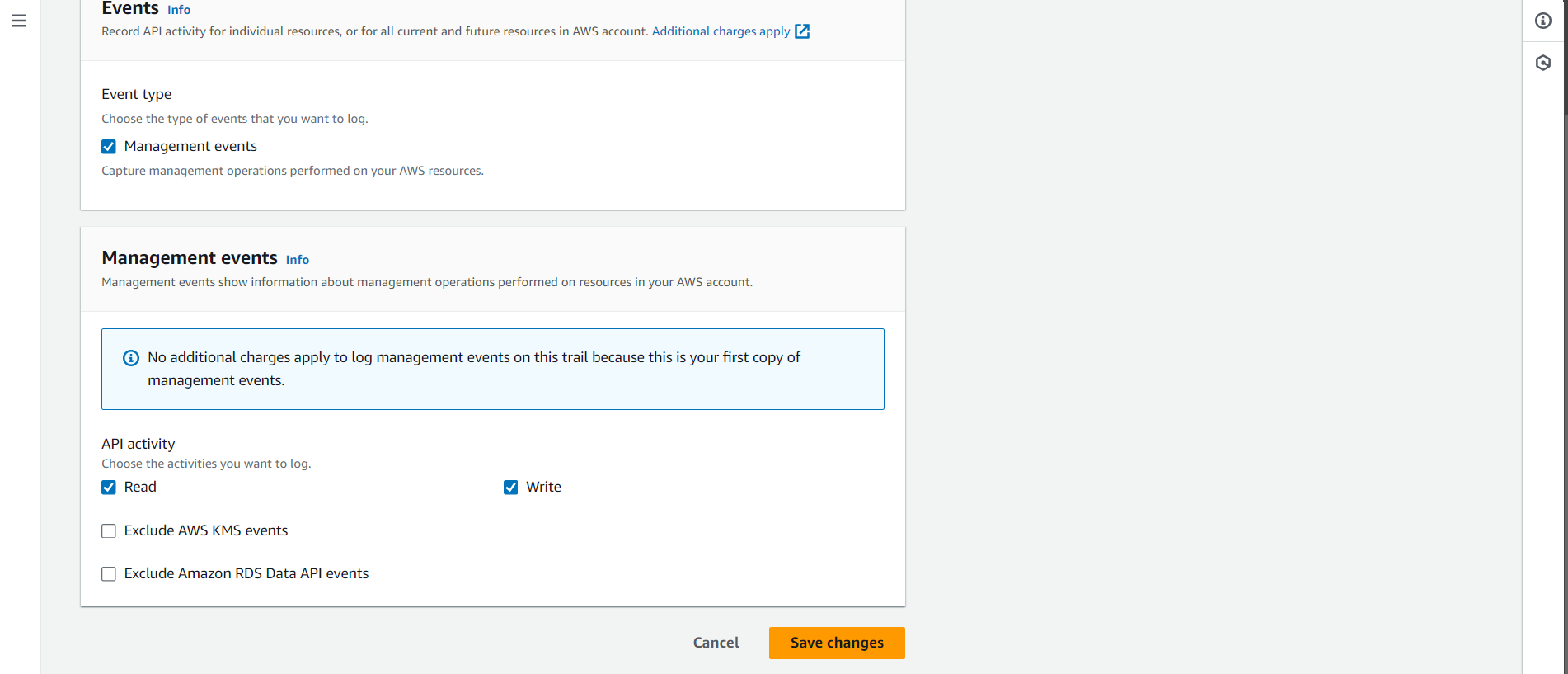


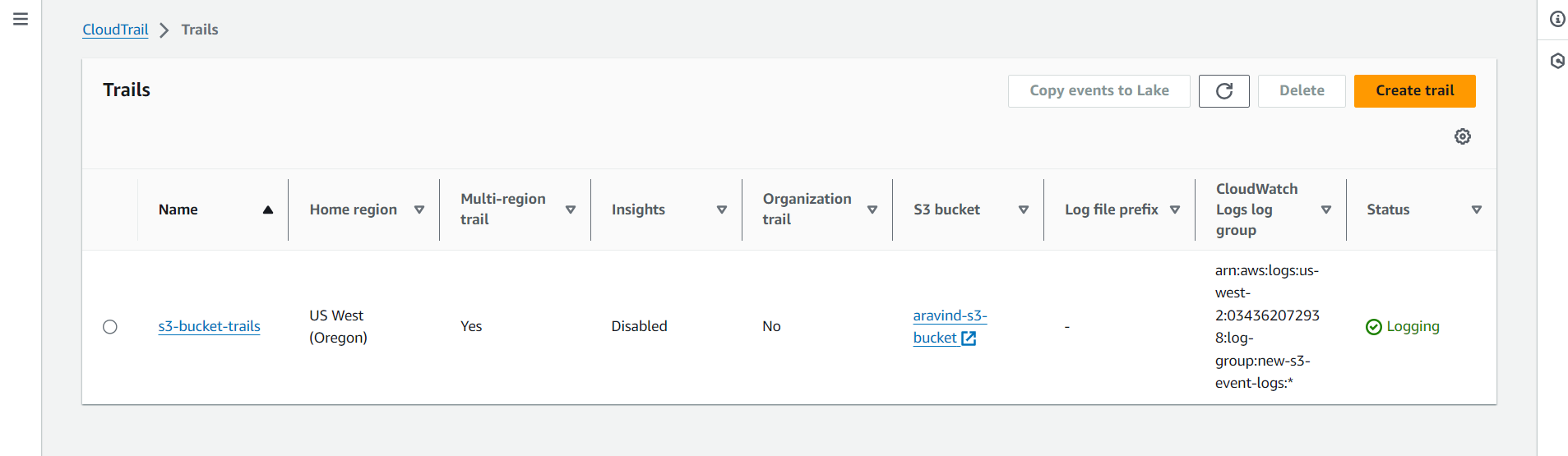
🡪Create CloudTrail for CloudWatch log group

CloudTrail 🡪 create trail 🡪 enter name 🡪 disable log file encryption 🡪 enable cloudwatch log 🡪 existing group 🡪 select group 🡪 select IAM role 🡪 next 🡪 management group 🡪 enable read and write 🡪 create trail

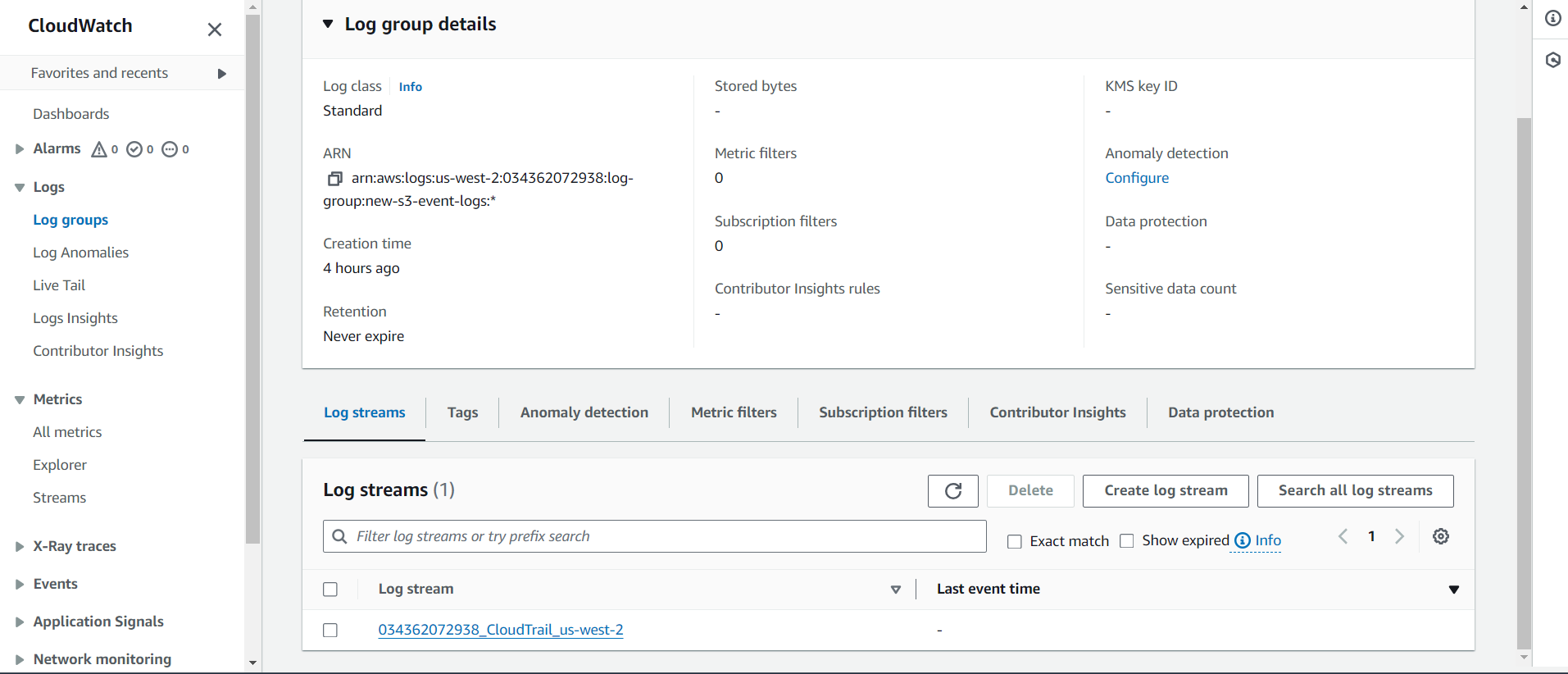




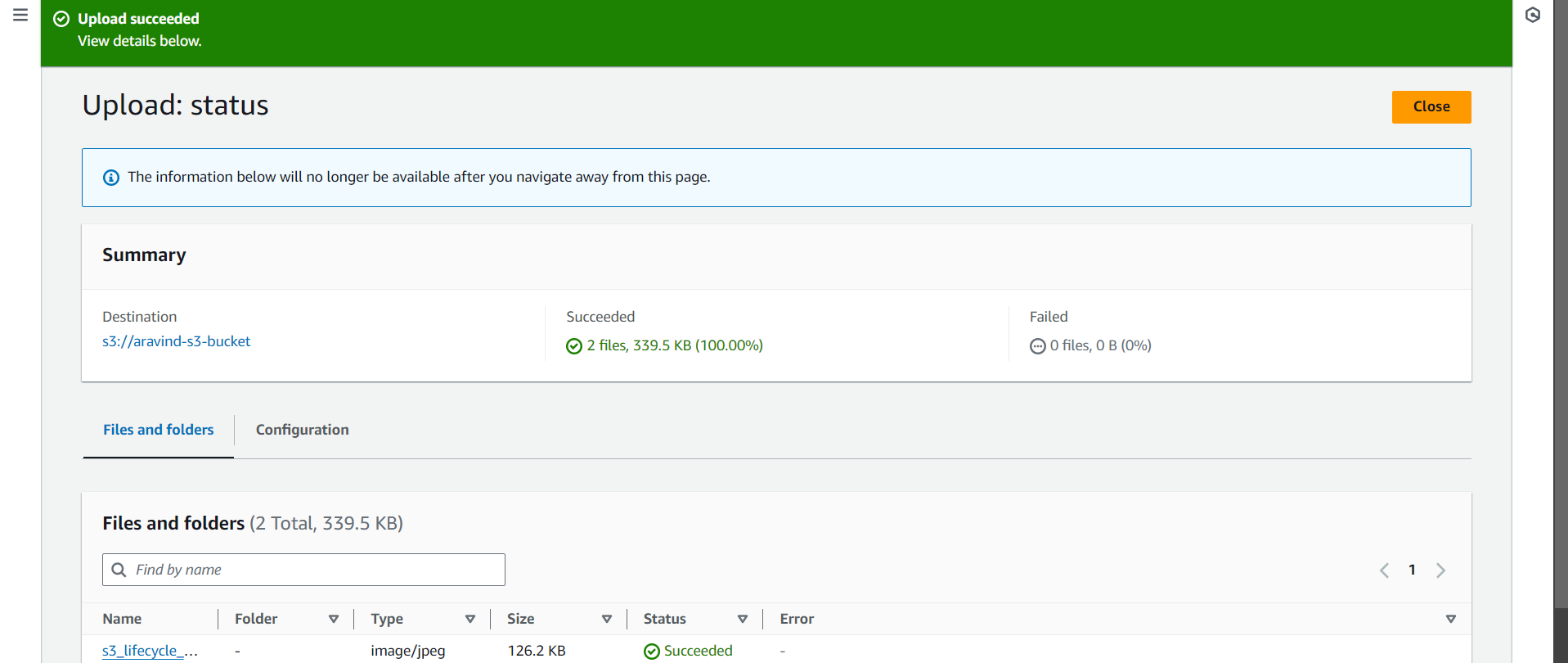




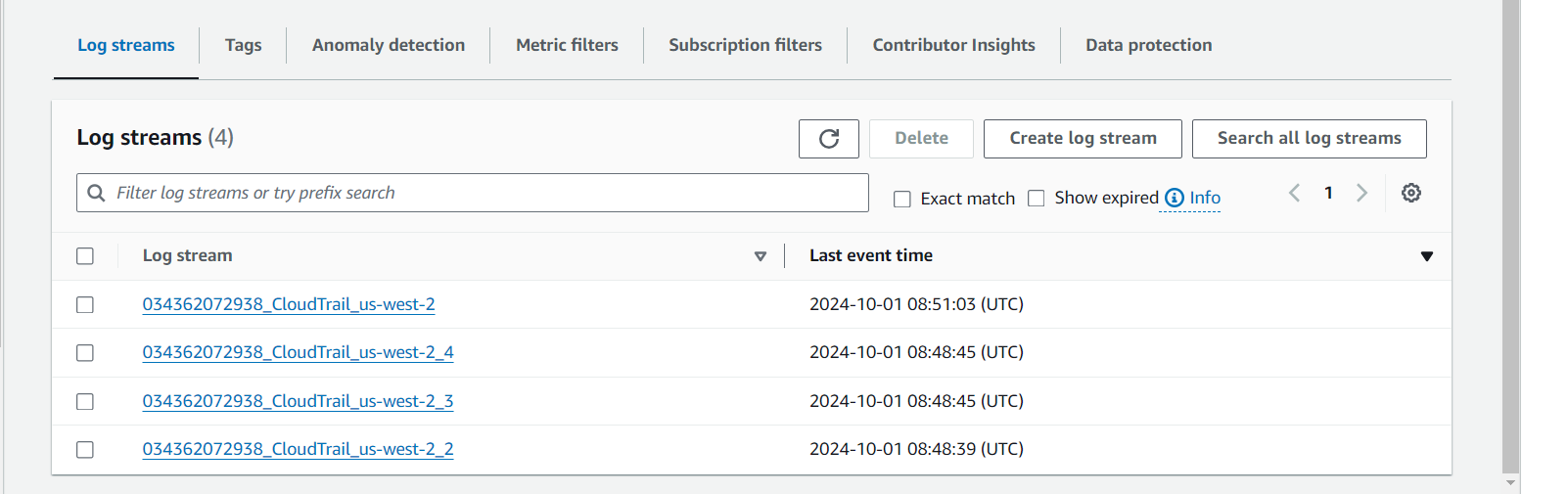
🡪Cloud Trail log stream

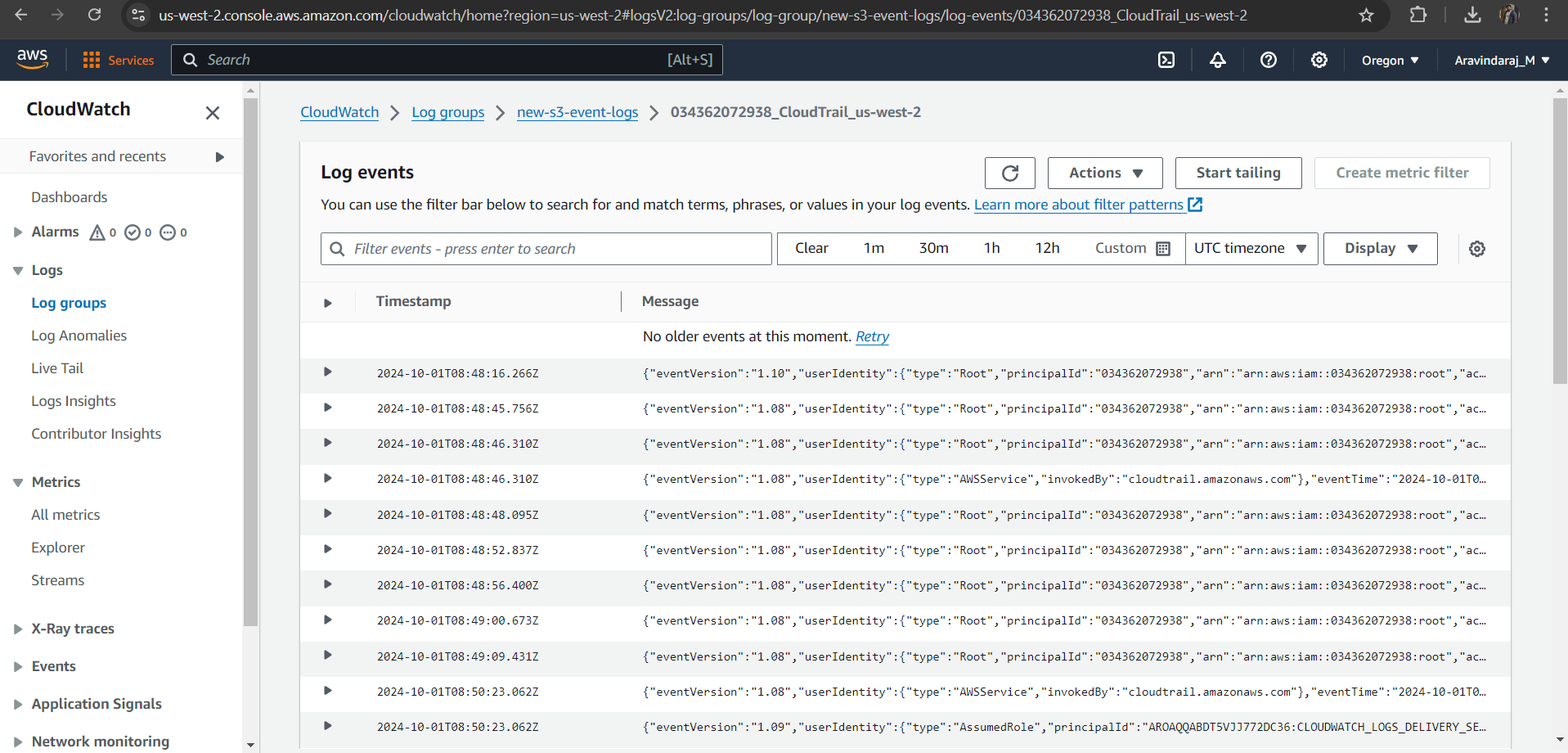


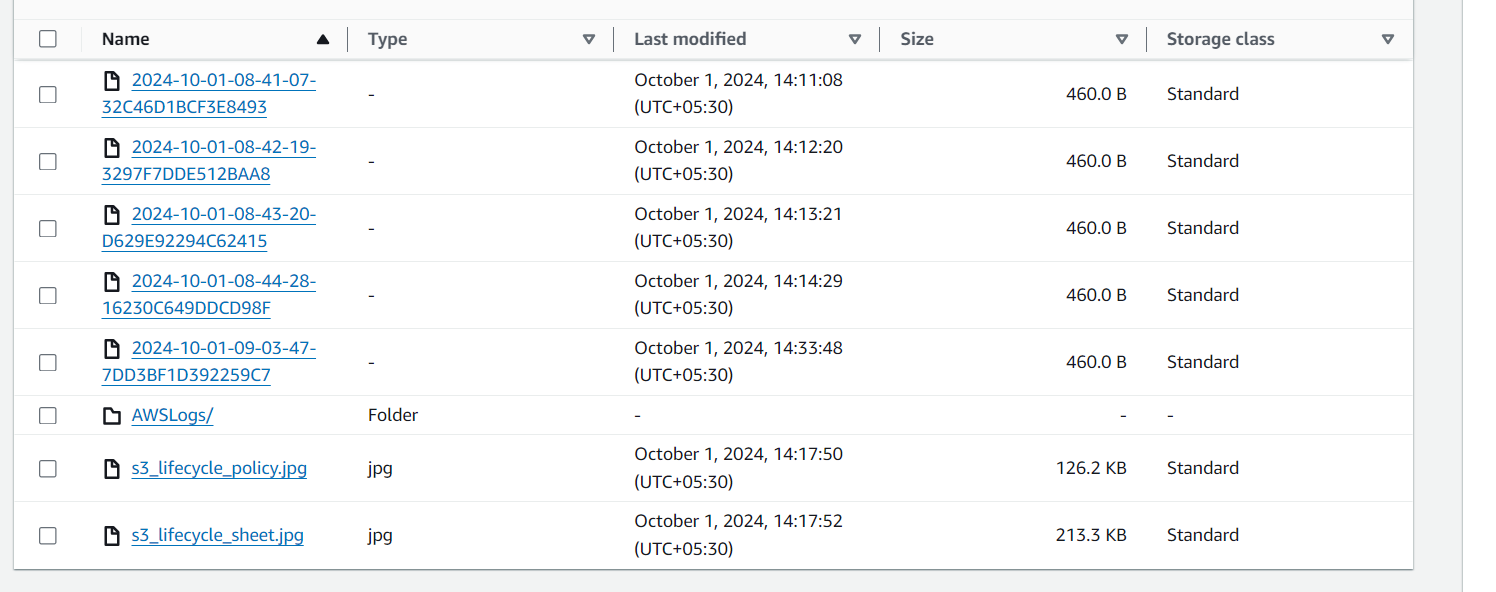
🡪Files uploaded to S3 bucket

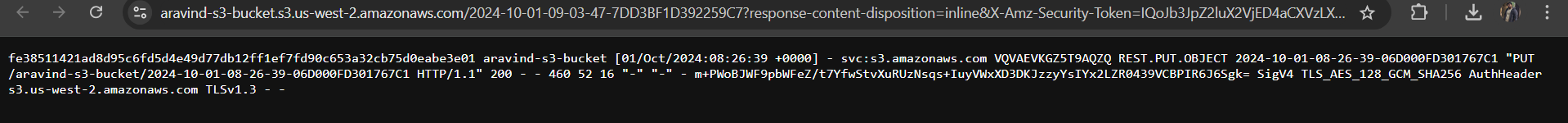


🡪Event Logs under Cloud Watch



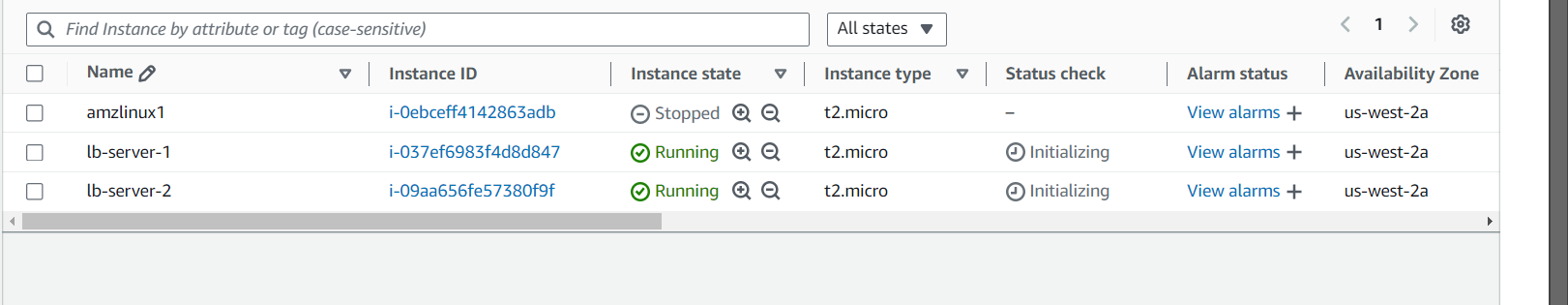


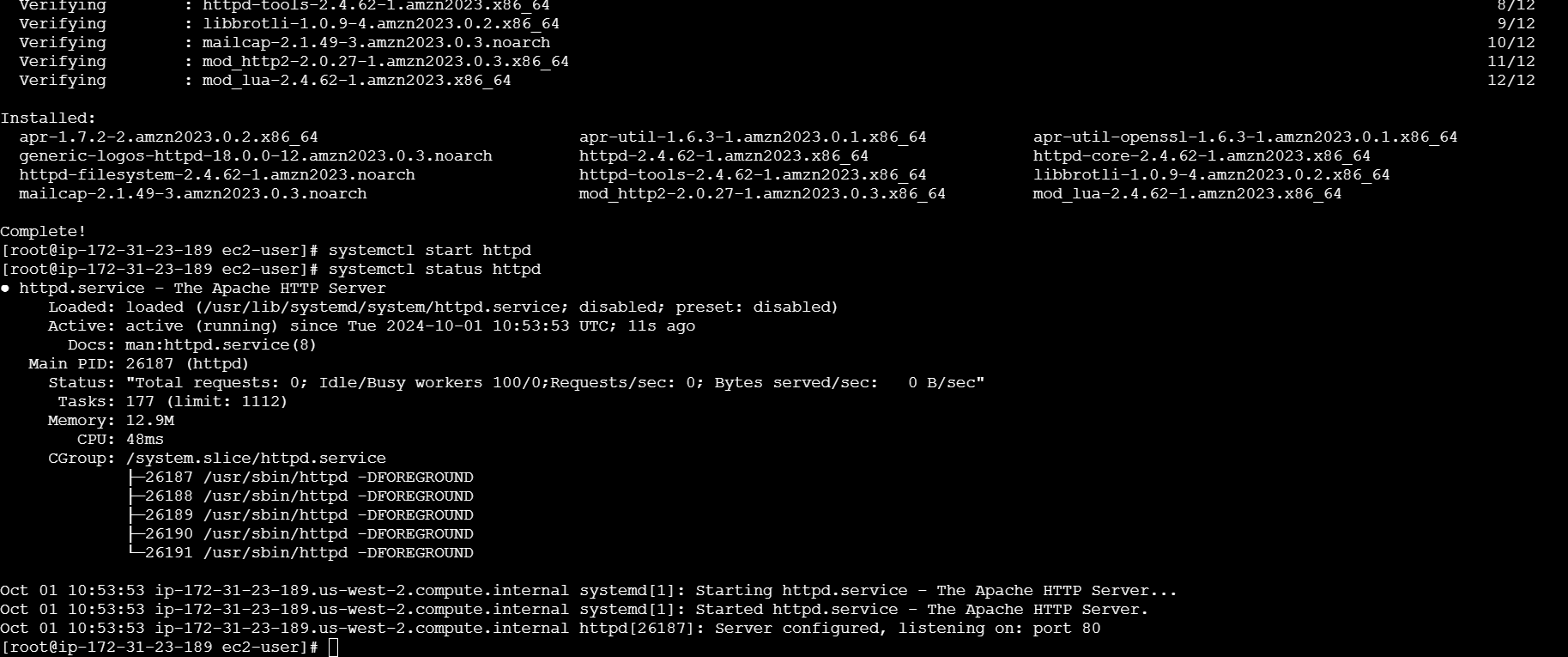




**2. Launch two ec2-instances and connect it to an application load balancer, where the output traffic from the server must be a load balancer IP address**

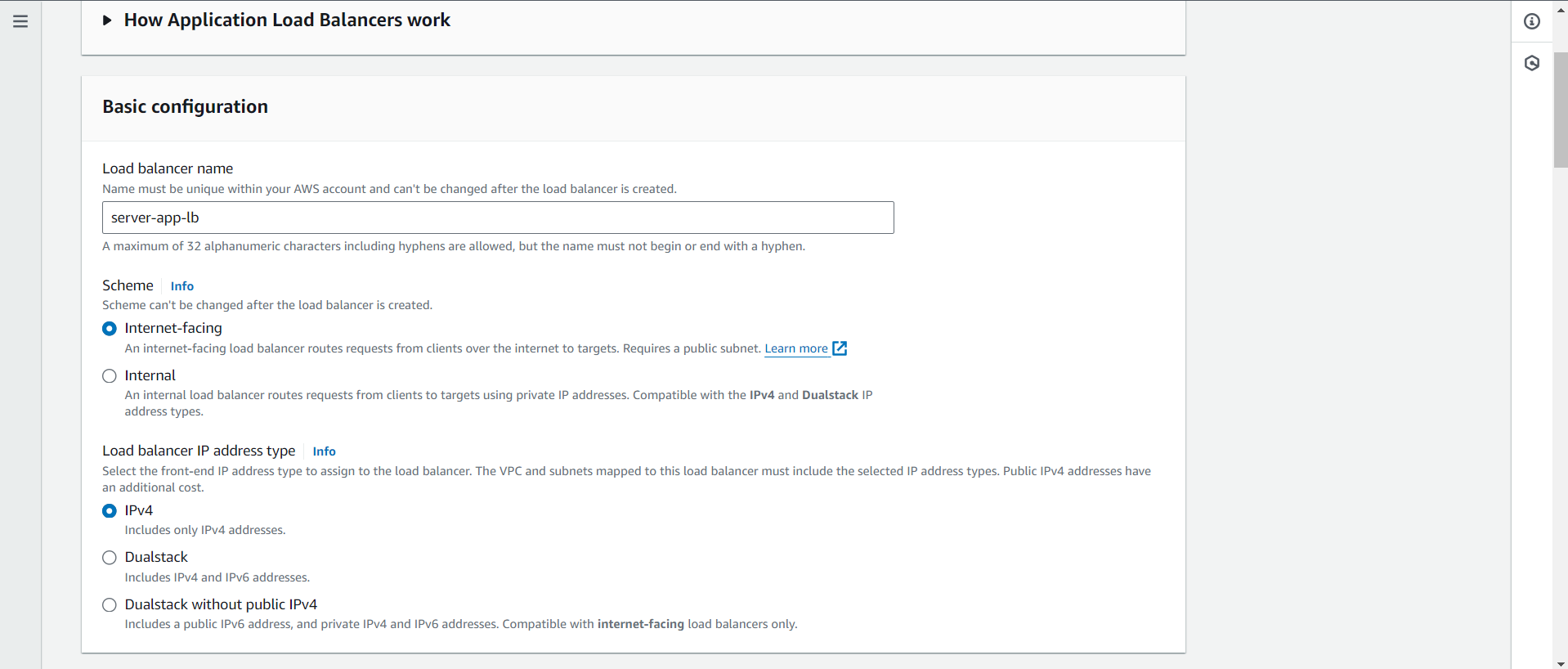
🡪Launching 2 EC2 instance with web server

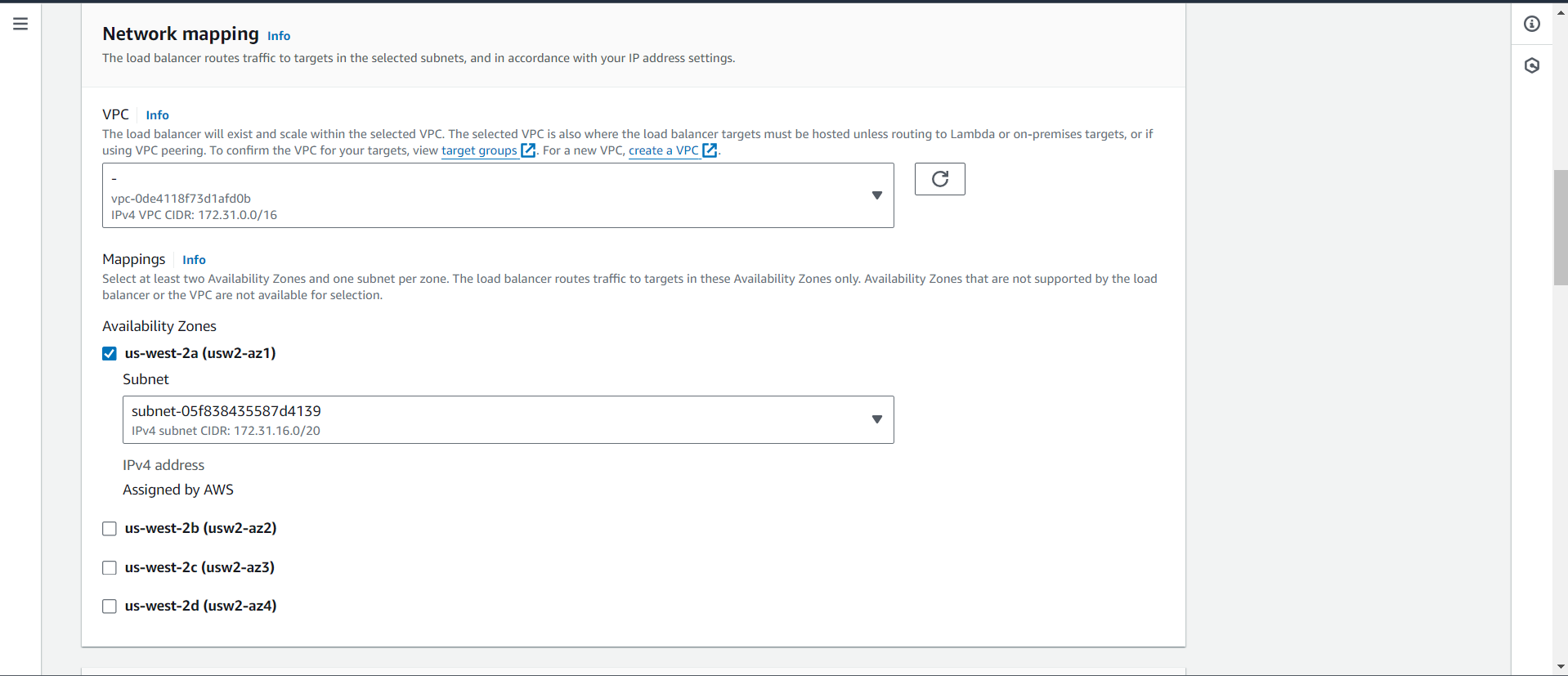


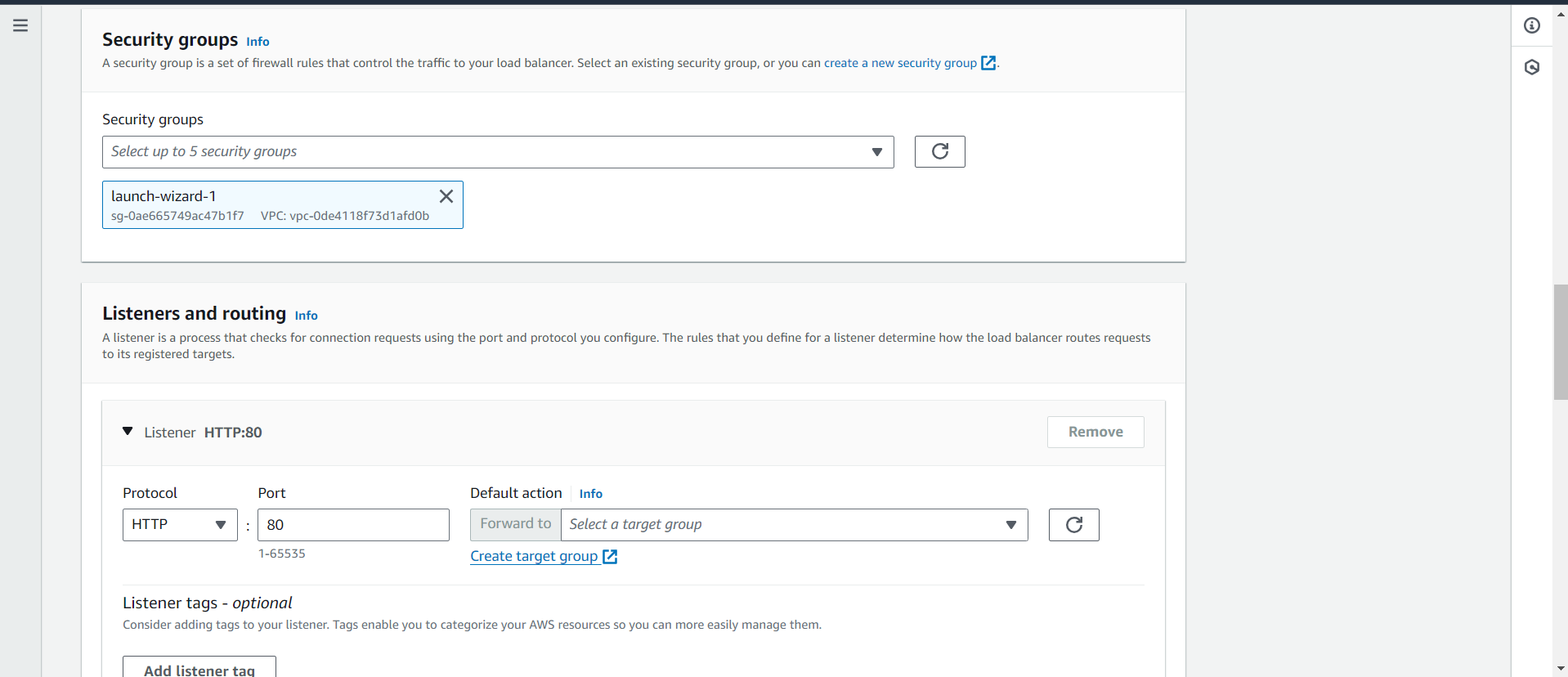


Load Balancer creation

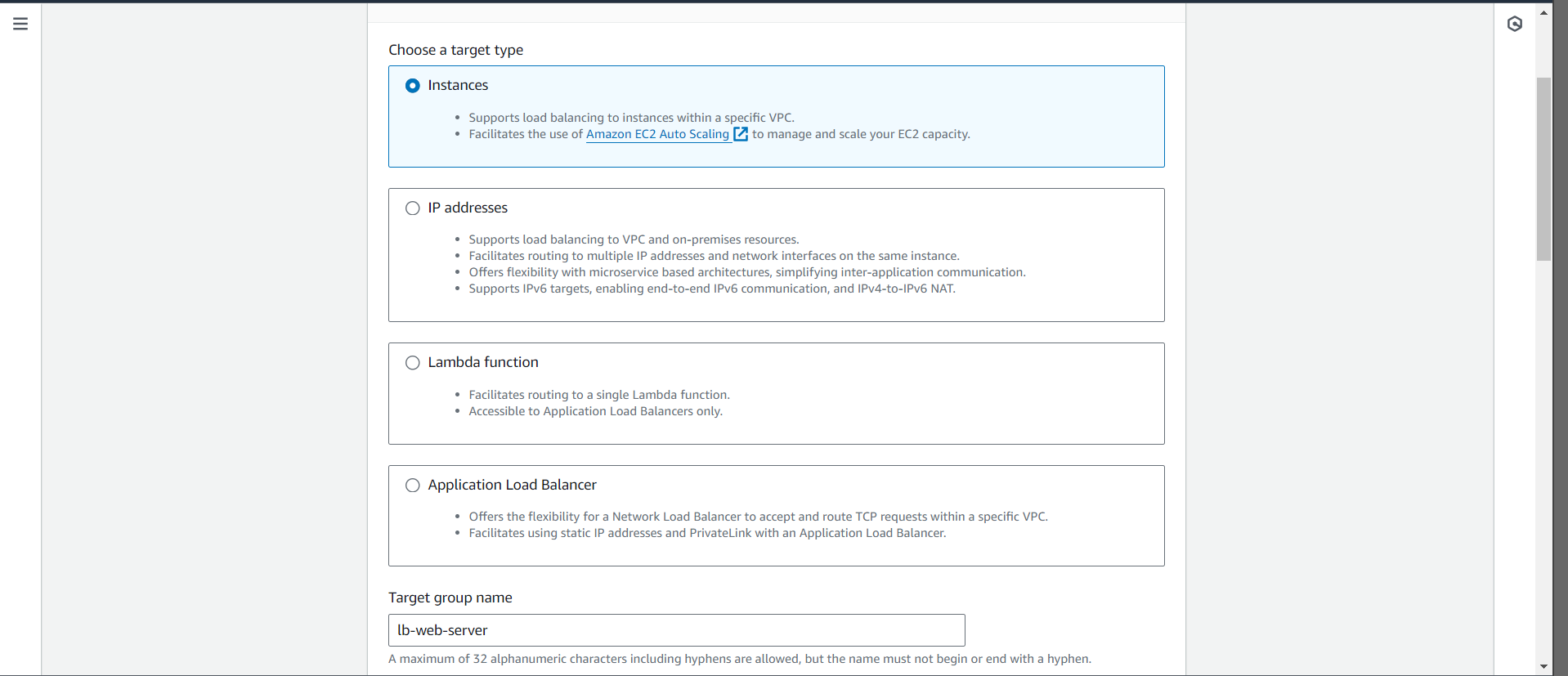
Load Balancer 🡪 Create Load Balancer 🡪 Application load balancer 🡪 enter name 🡪 select internet facing 🡪

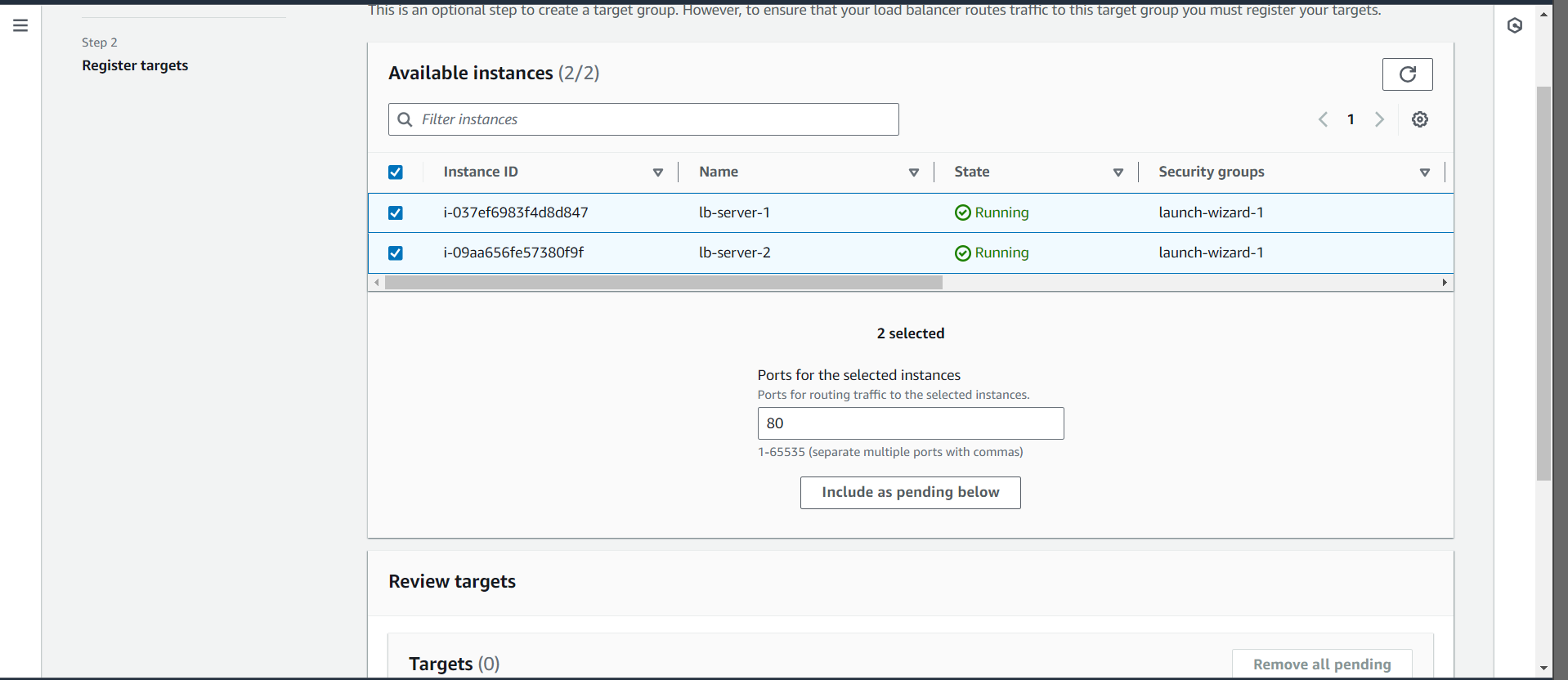


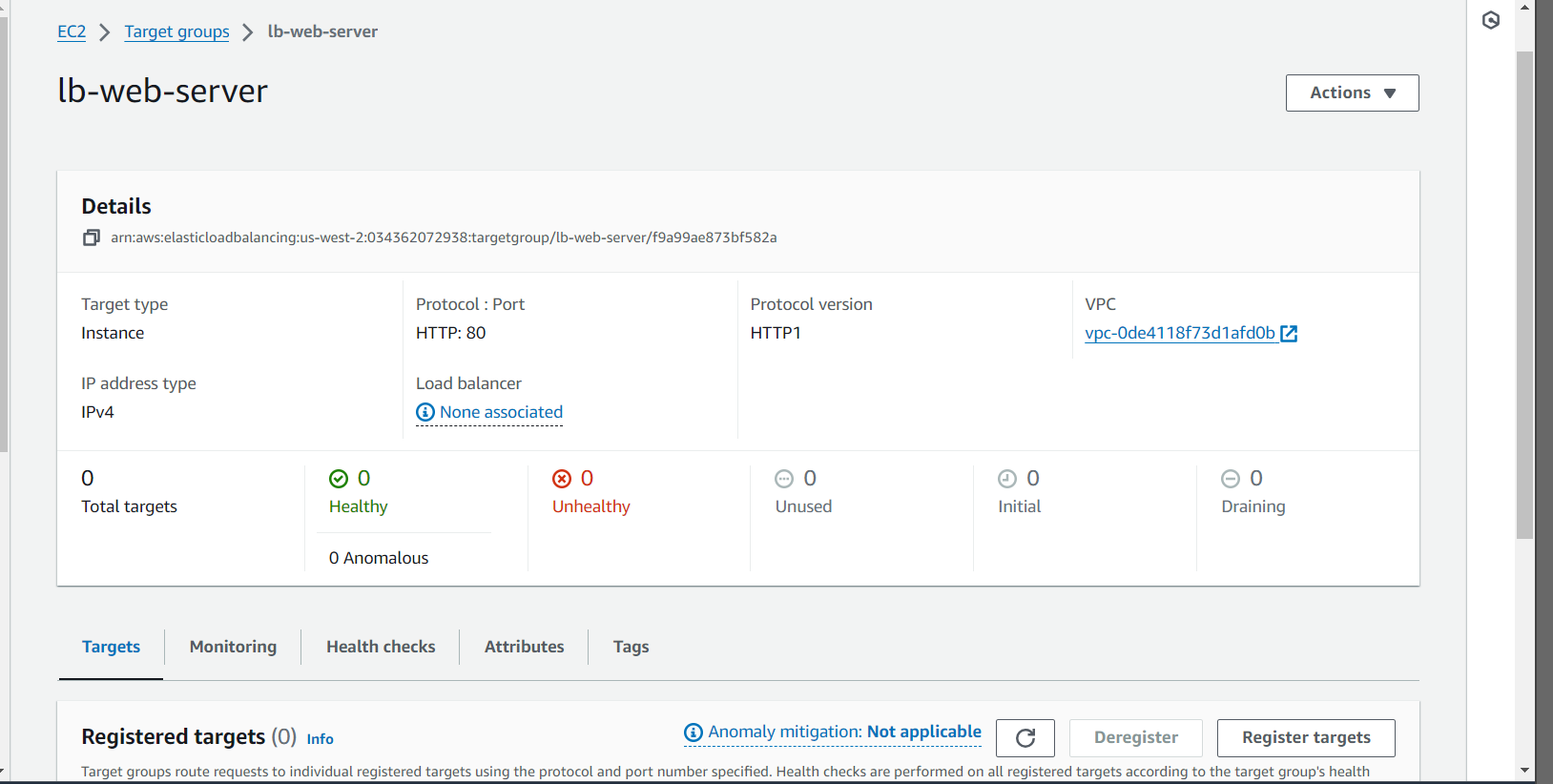




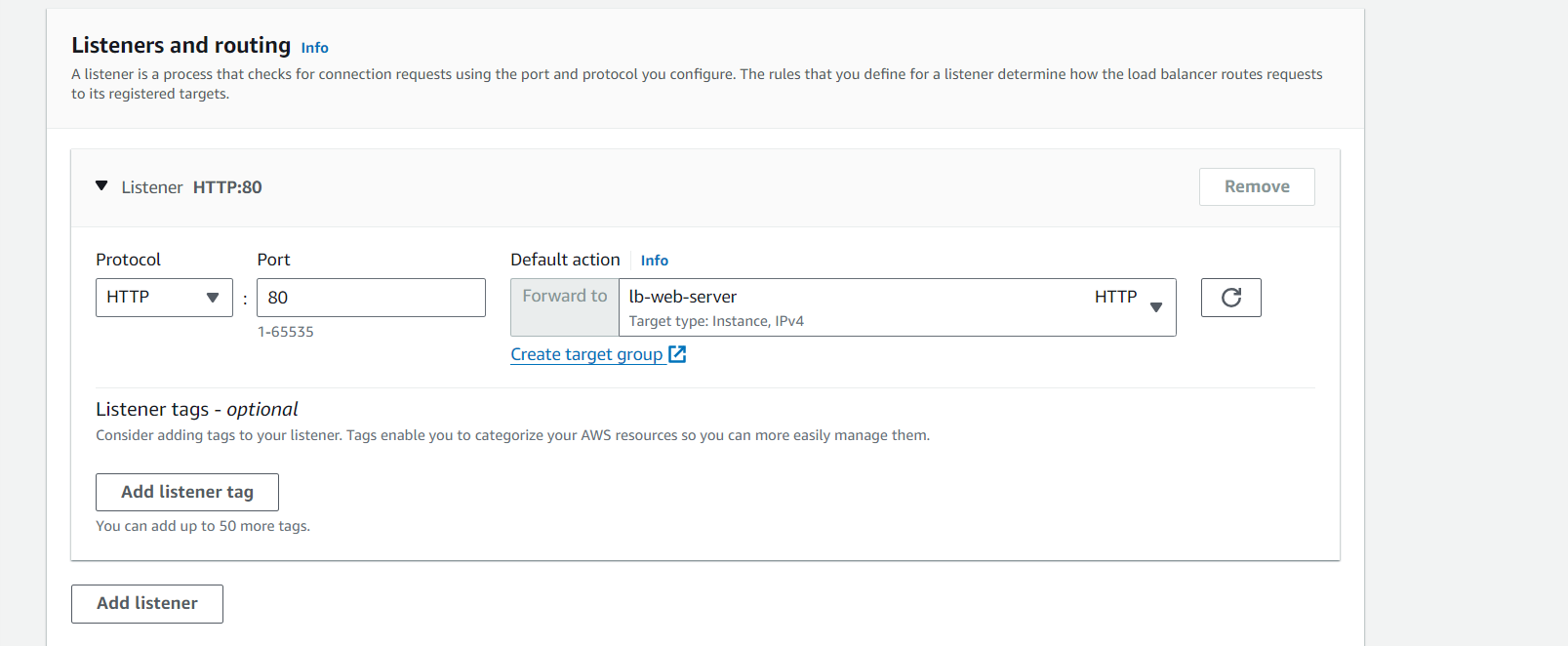
Create target group

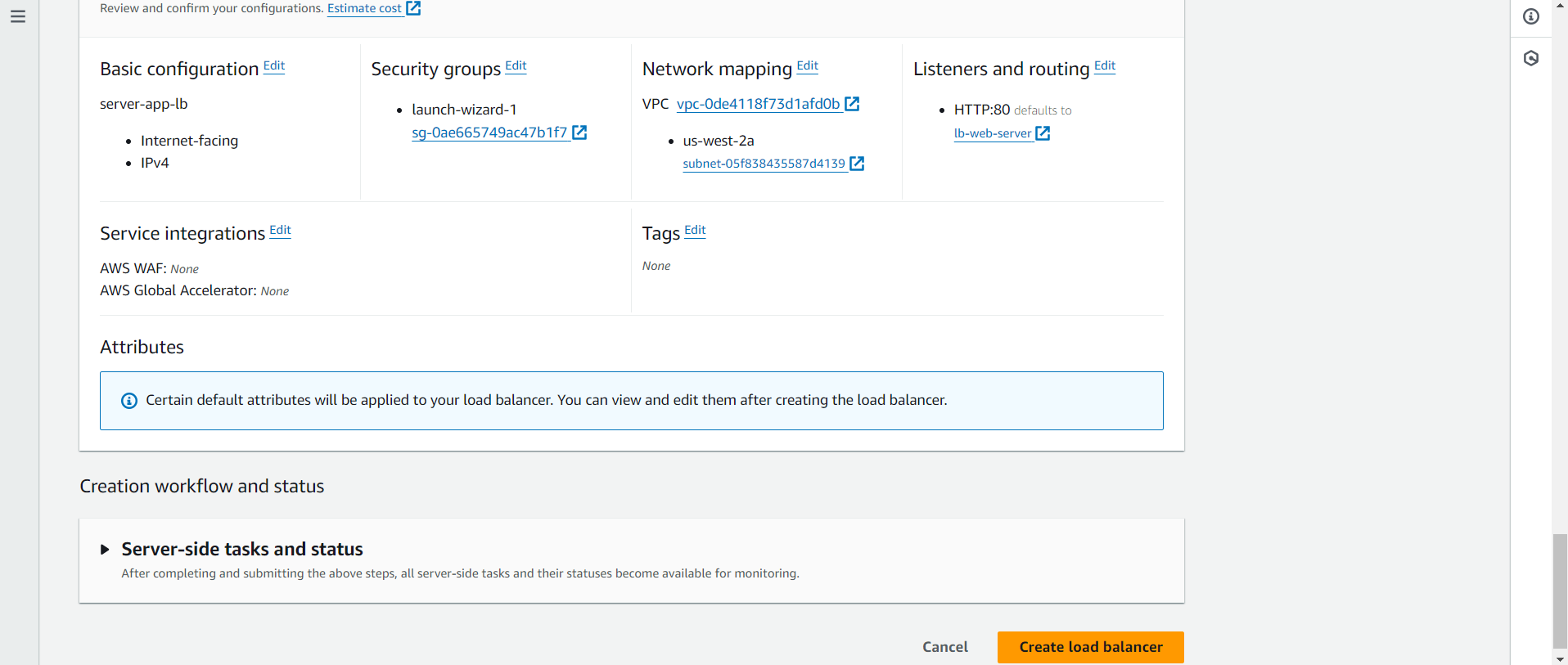


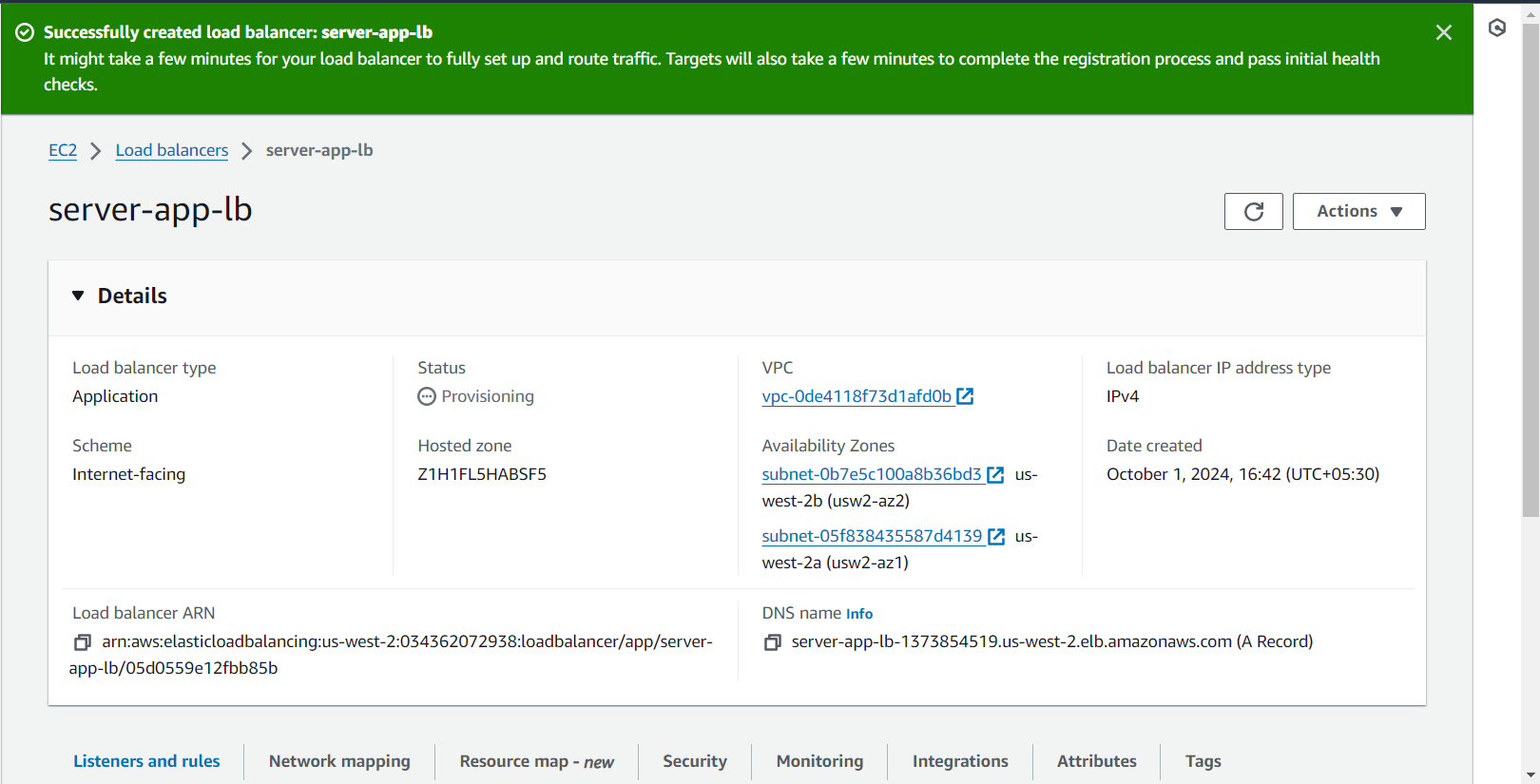




Select the Target Group in Load balancer







Use the Load Balancer DNS name to check the EC2 Web server

