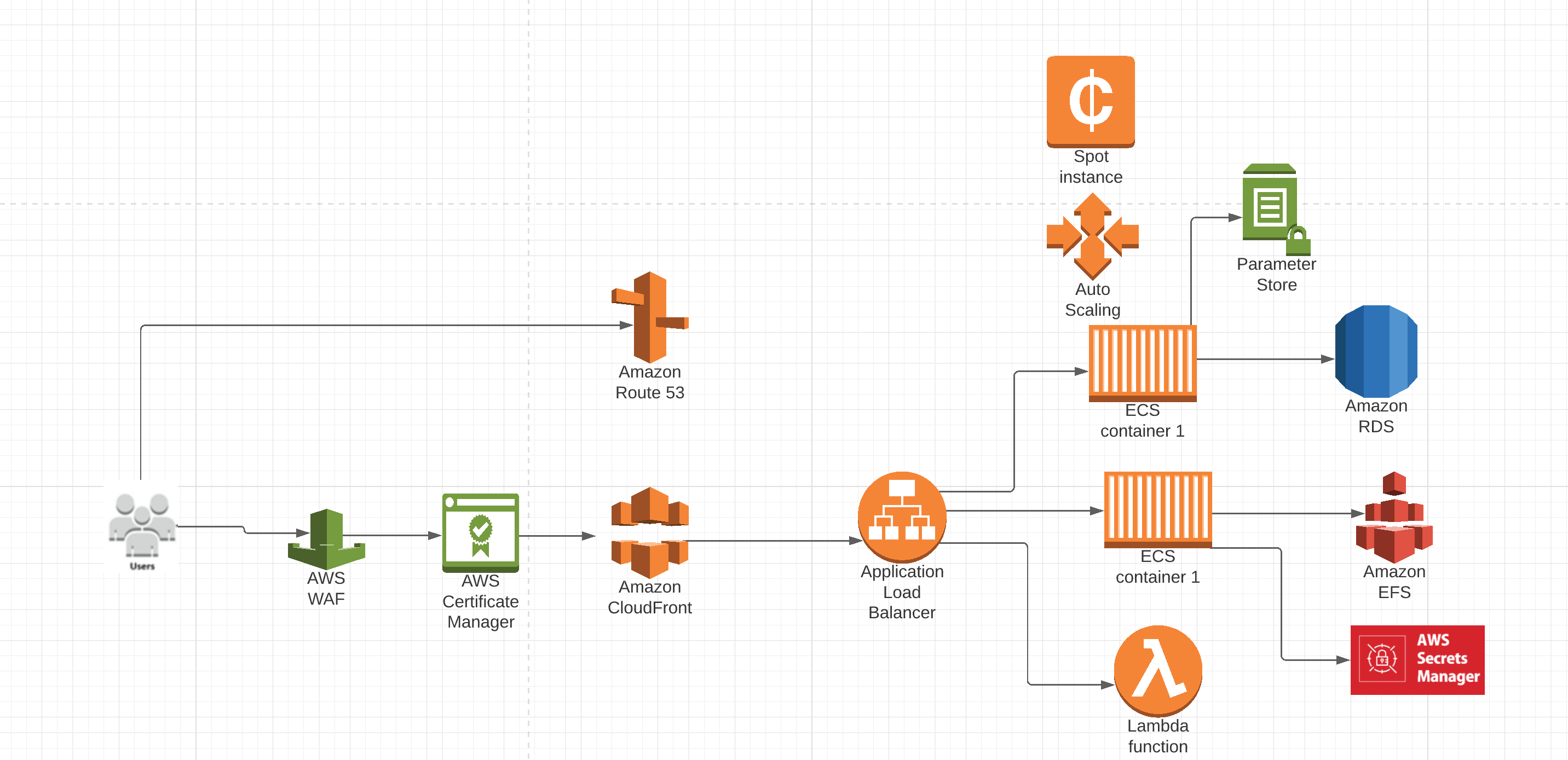
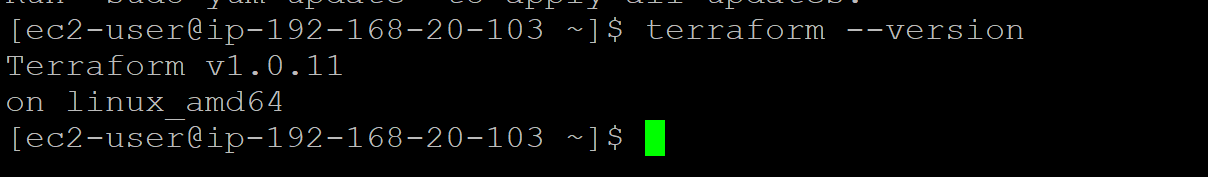
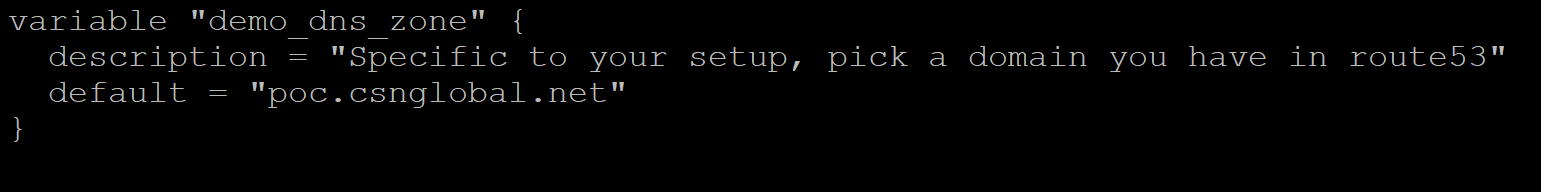
**Basic diagram as following**



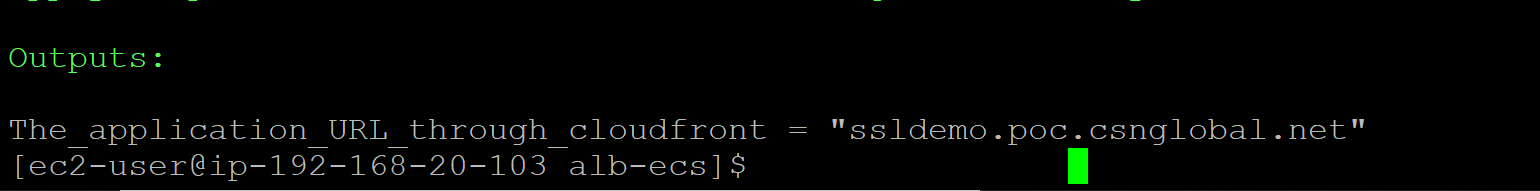
I used following terraform version



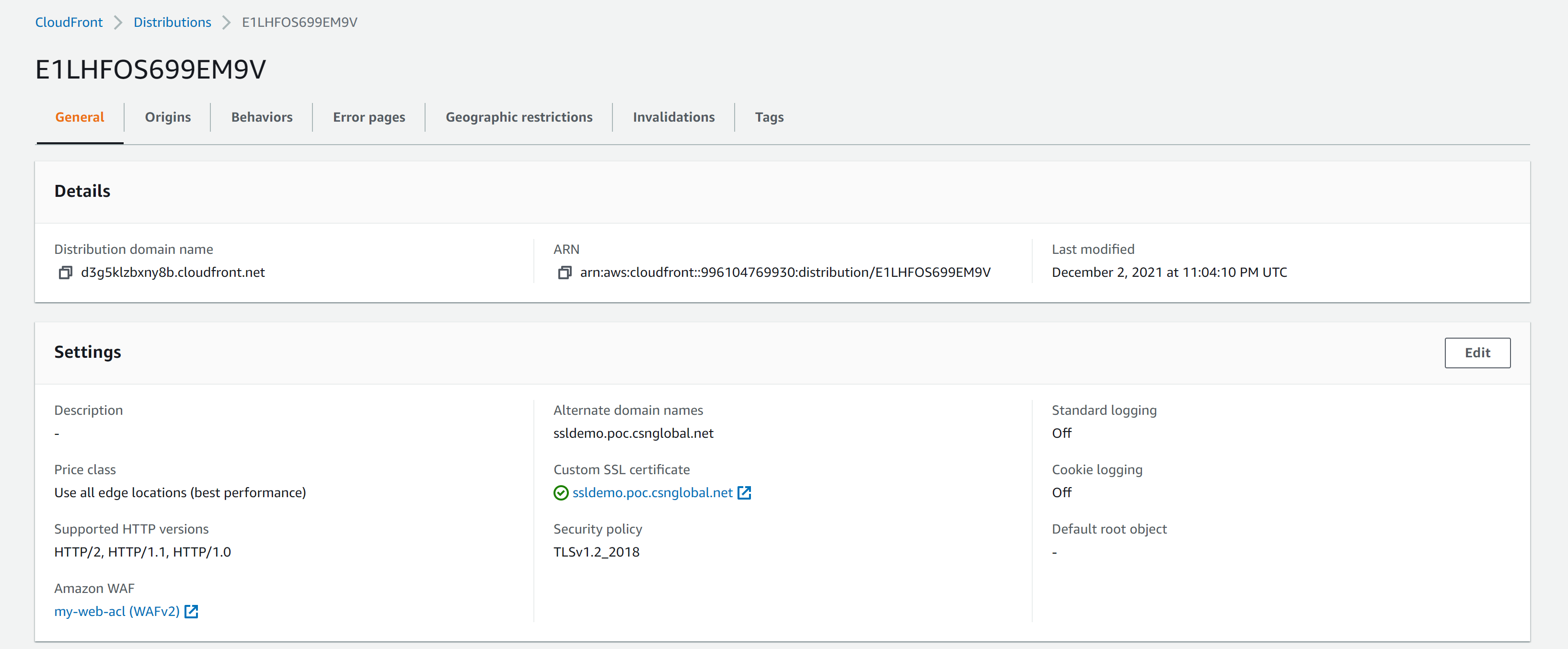
Please modify variables.tf file to change environment variable, most of variables can use default value, the one need change is demo\_dns\_zone, must be one AWS account registered Route53 zone.



Terraform will output Cloudfront alias URL



Cloudfront configuration as following, origin is ALB (path based route, default region is ap-southeast-2) and protected by WAFv2, ACM of us-east-1 for cloudfront

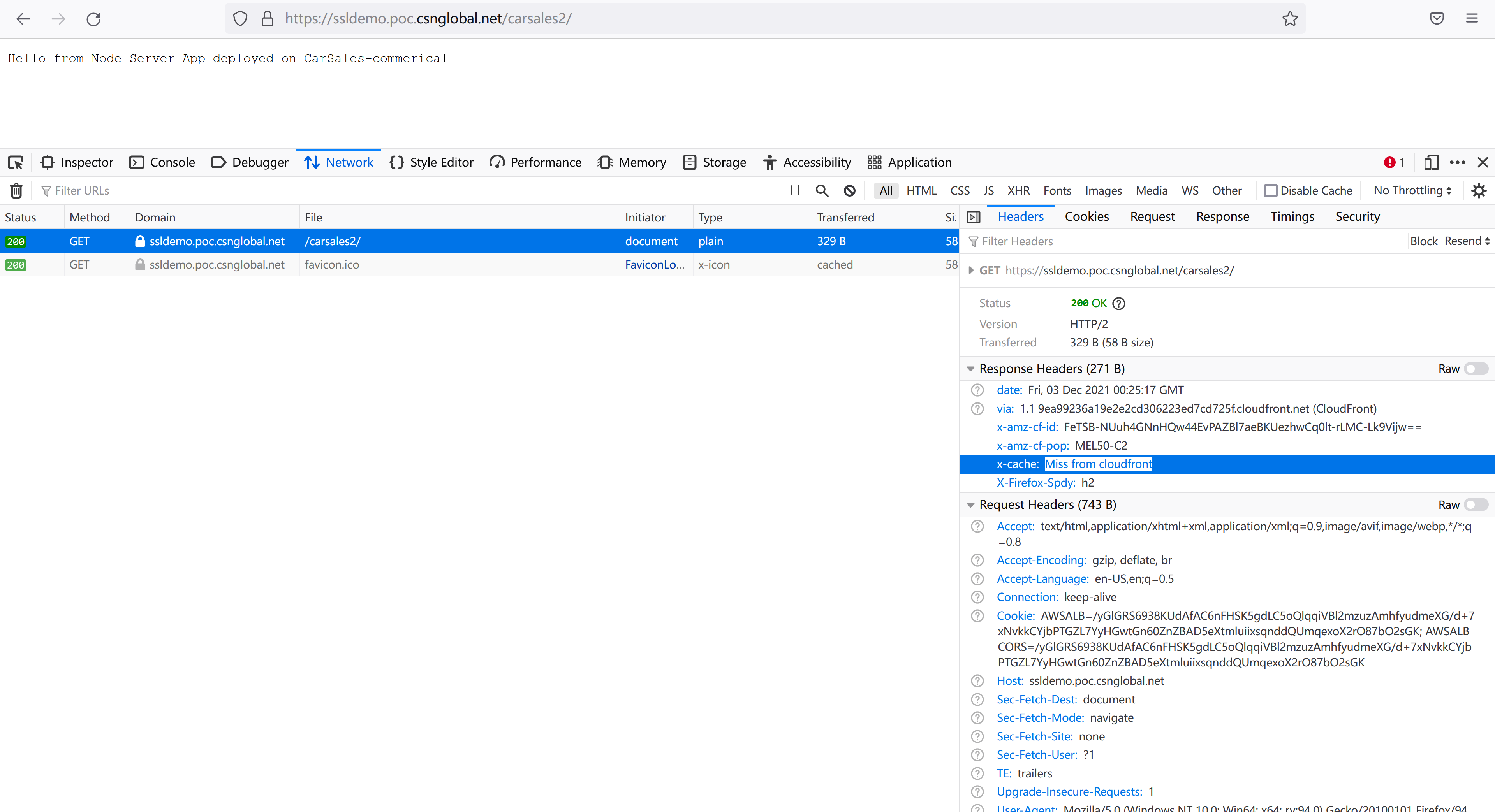


https://ssldemo.poc.csnglobal.net/carsales1/

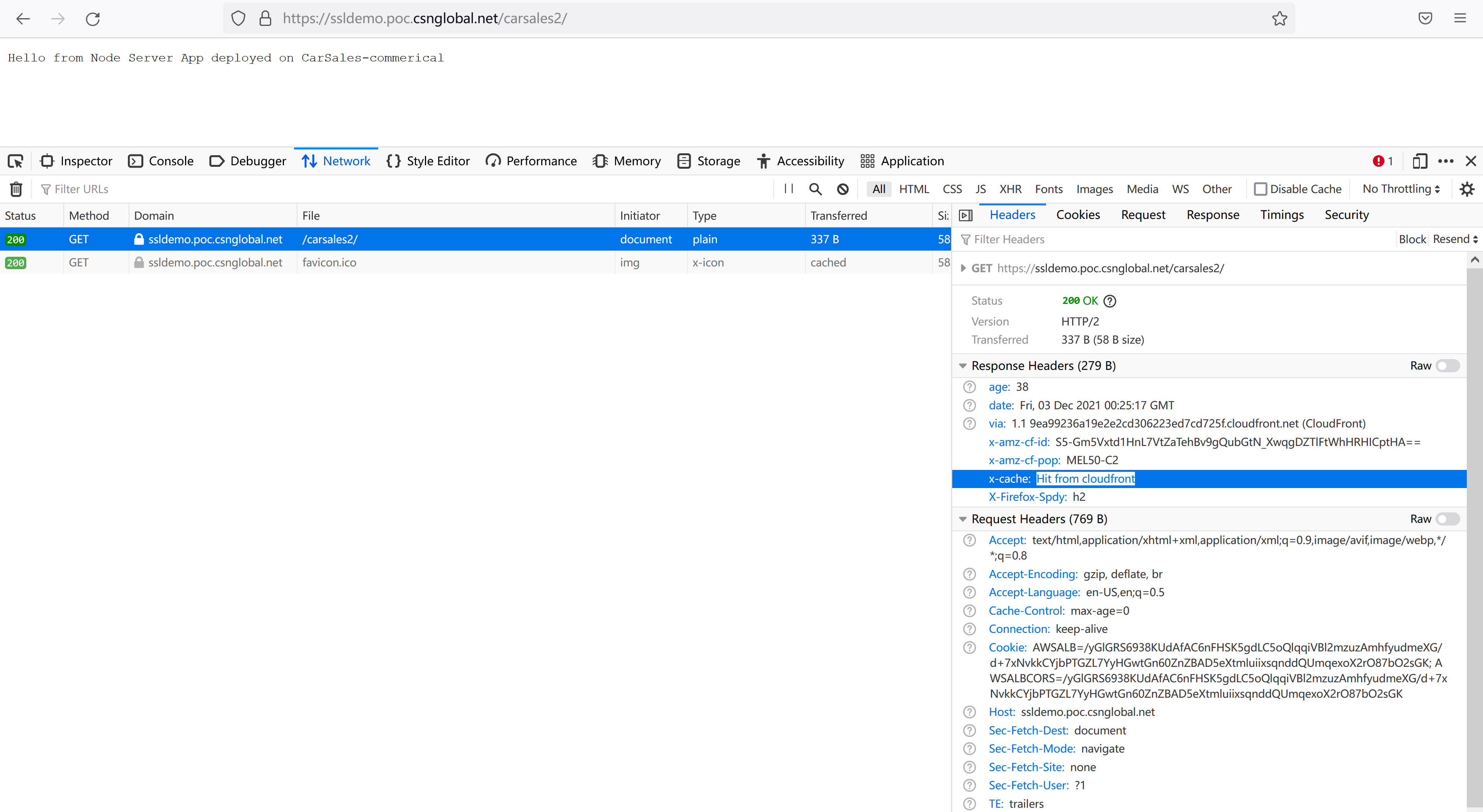
https://ssldemo.poc.csnglobal.net/carsales2/

https://ssldemo.poc.csnglobal.net/lambda/

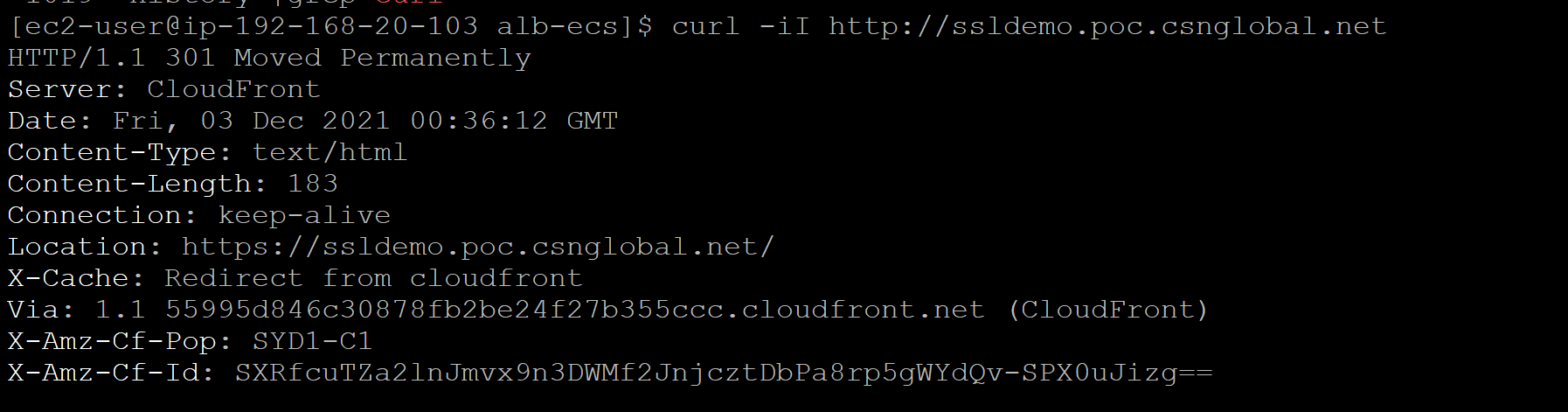
When you first open one url ,check network information, it will show miss from cloudfront,



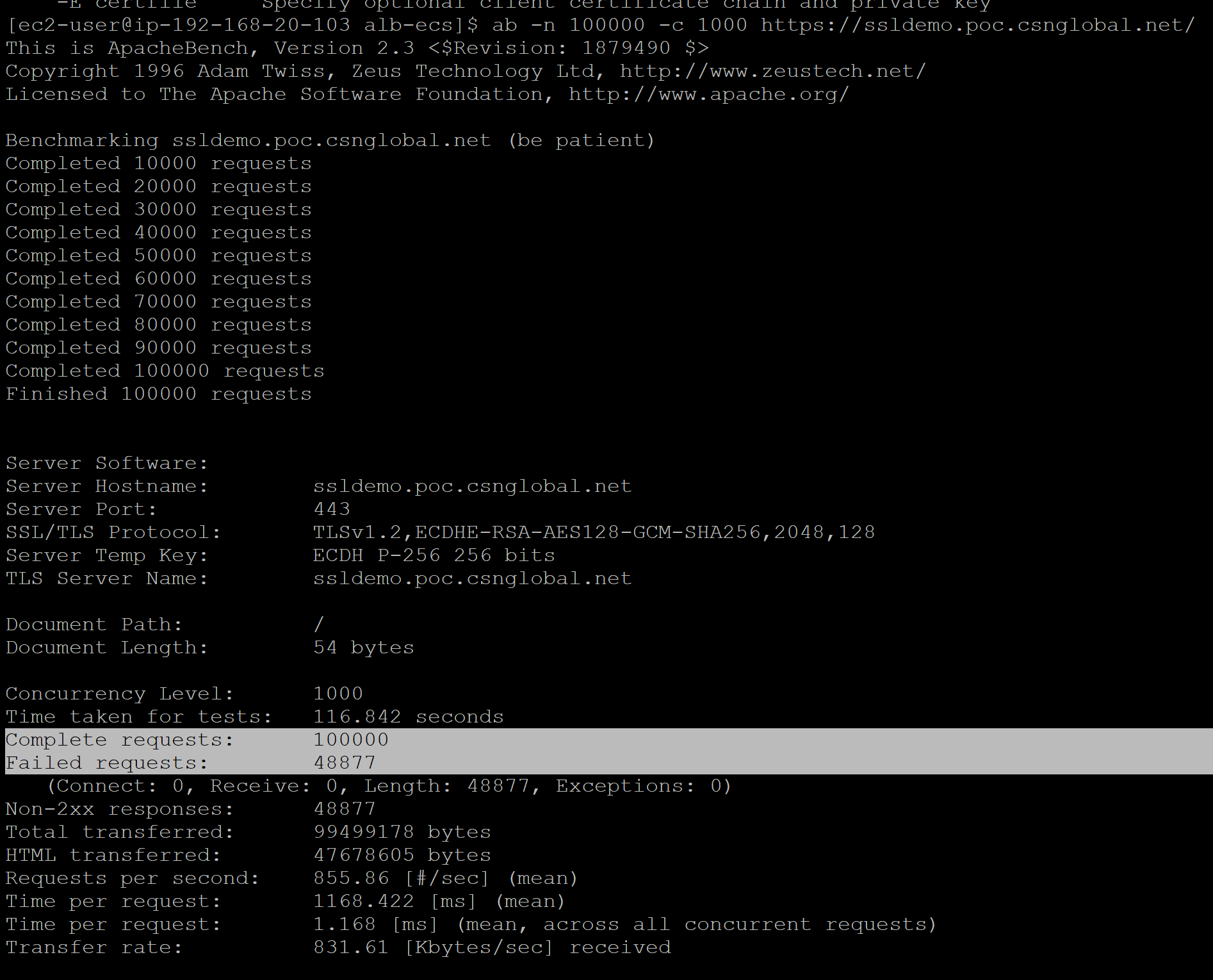
When you refresh the page again, it will show hit from cloudfront.

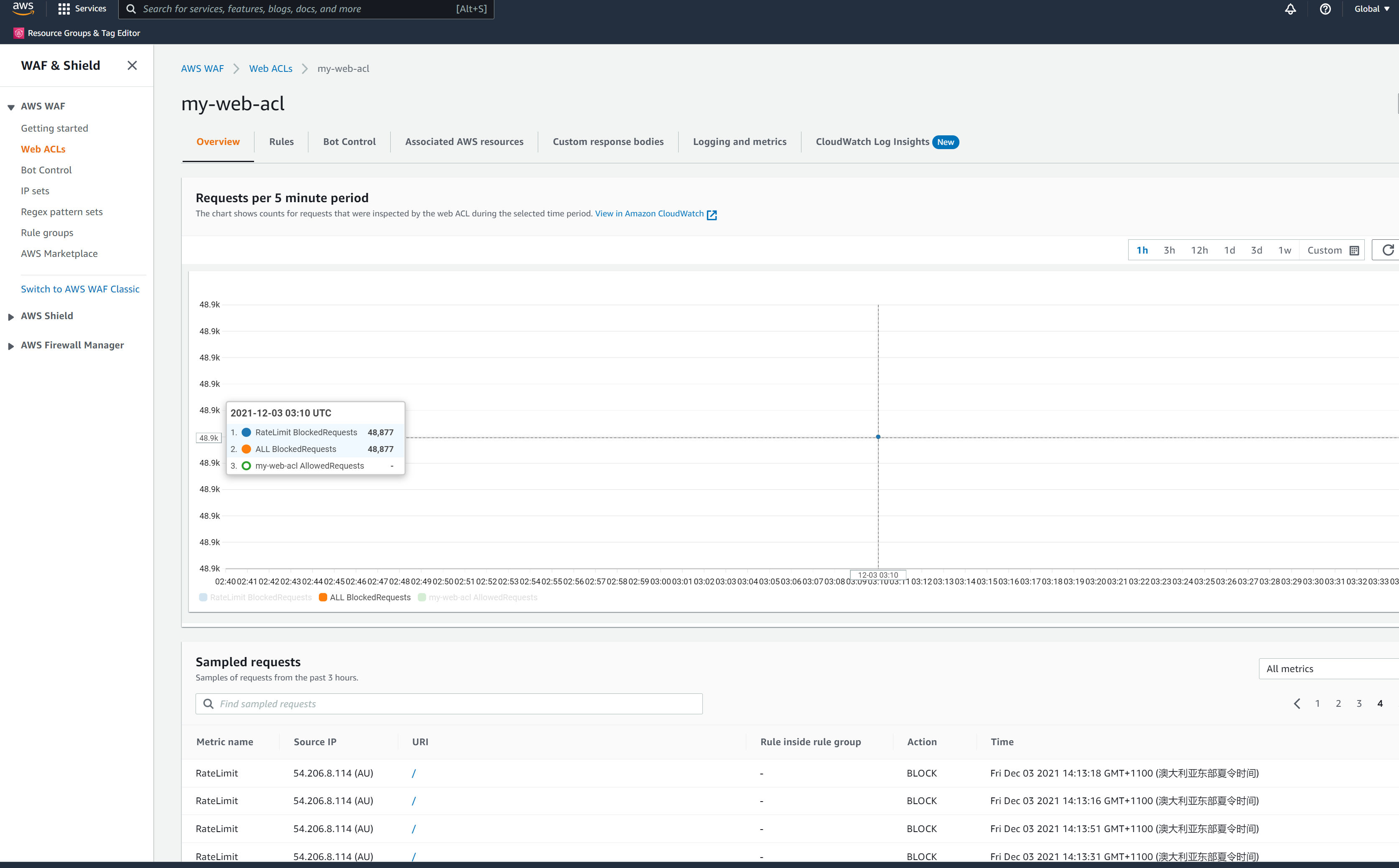


When check http of cloudfront url(. curl -iI http://ssldemo.poc.csnglobal.net) , it will redirect to https

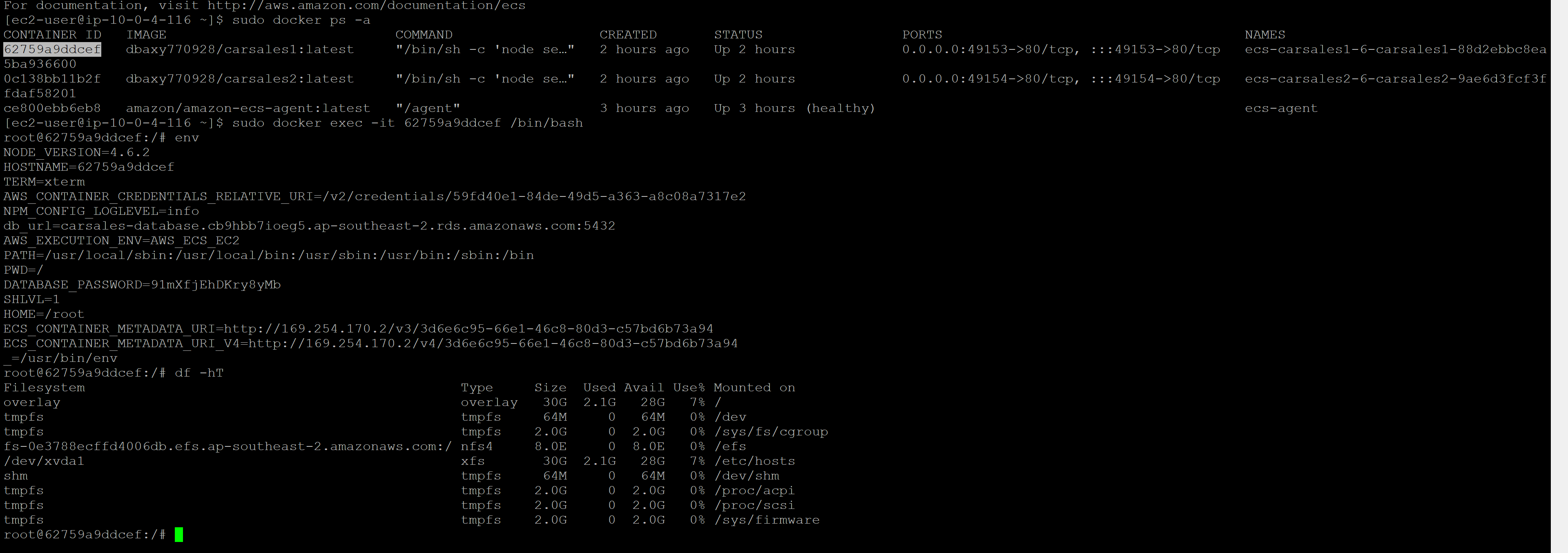


Cloudfront is protected by WAF, it has one Web ACL name my-web-acl that rate limit. We can use ab tool to simulate huge traffic from one single IP to verify WAF will block the repeated traffic.from command line output, we find failed request is 48877, same with AWS WAF result.

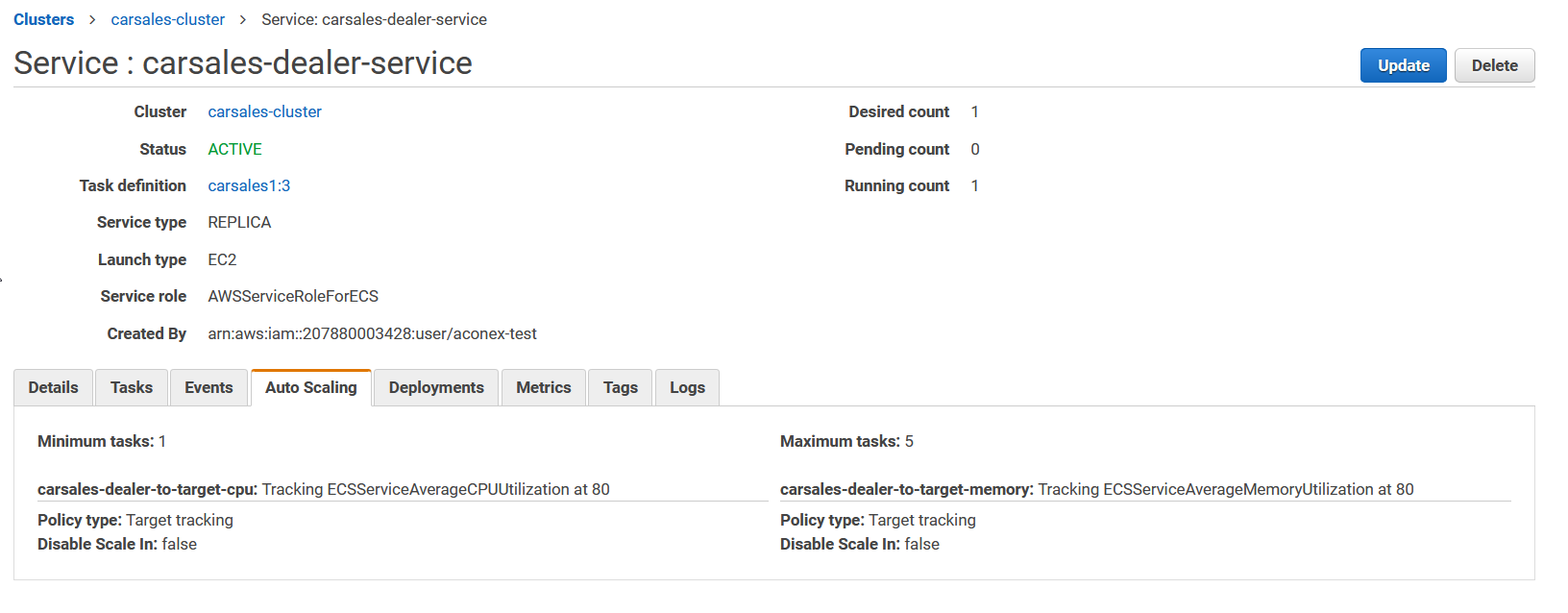




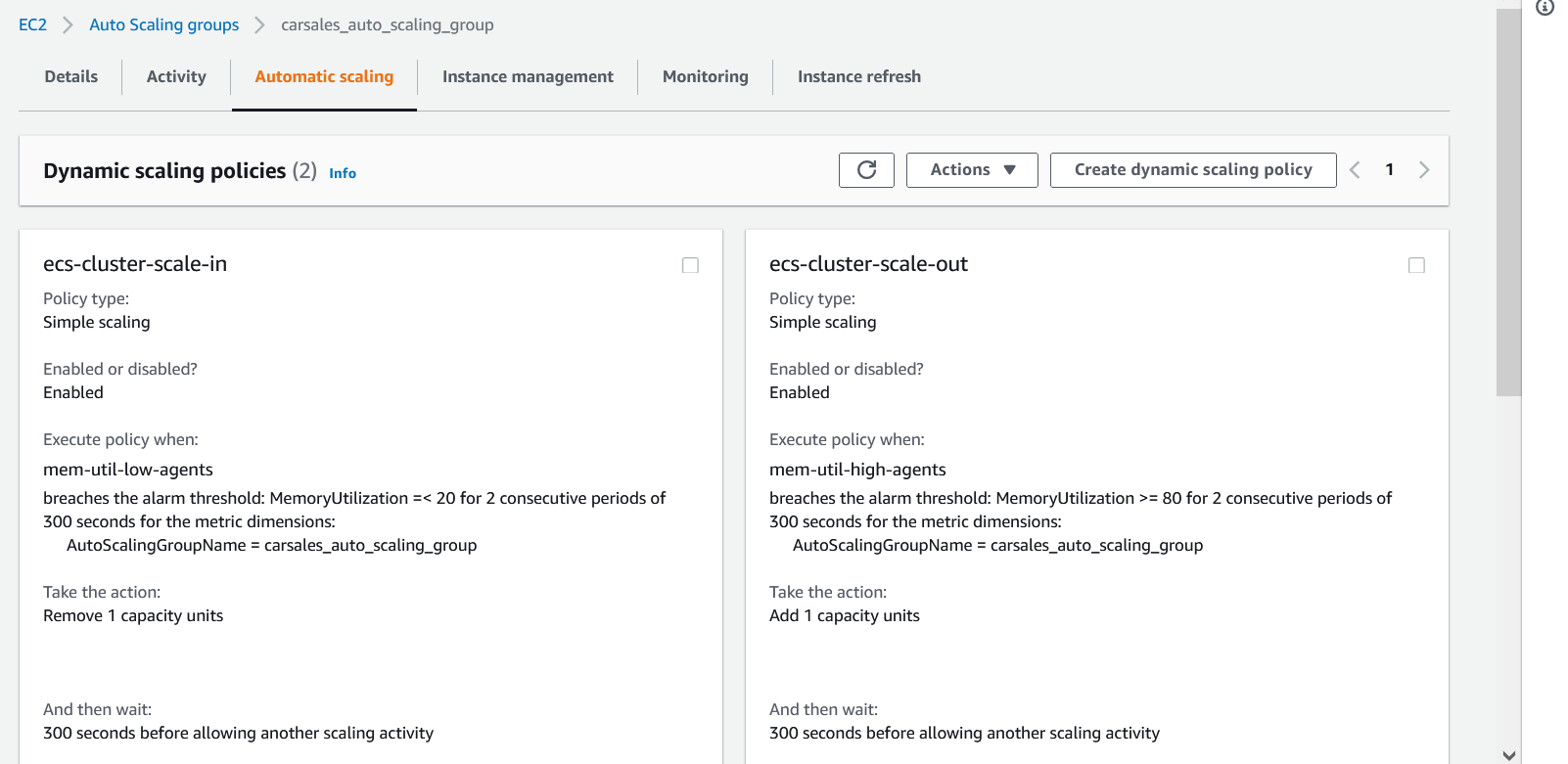
Access ECS EC2 instance from bastion host. Login to container and check command env output (you can find RDS db\_url and RDS database password which can be used to access database from docker container if application needed ) and df -hT (EFS mount) to store data outside in case docker container scale in or docker container crash.



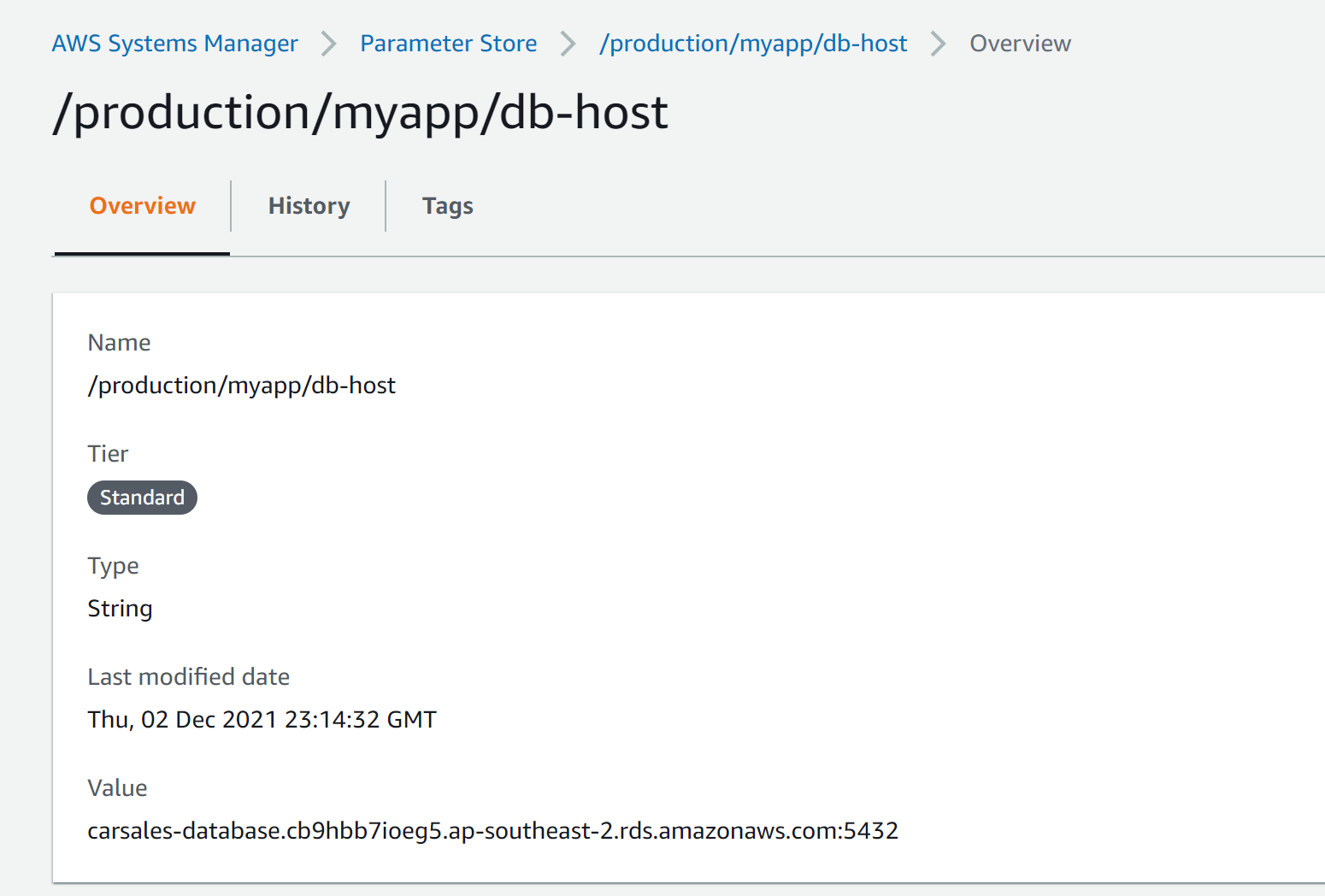
* ECS service autoscale based on load



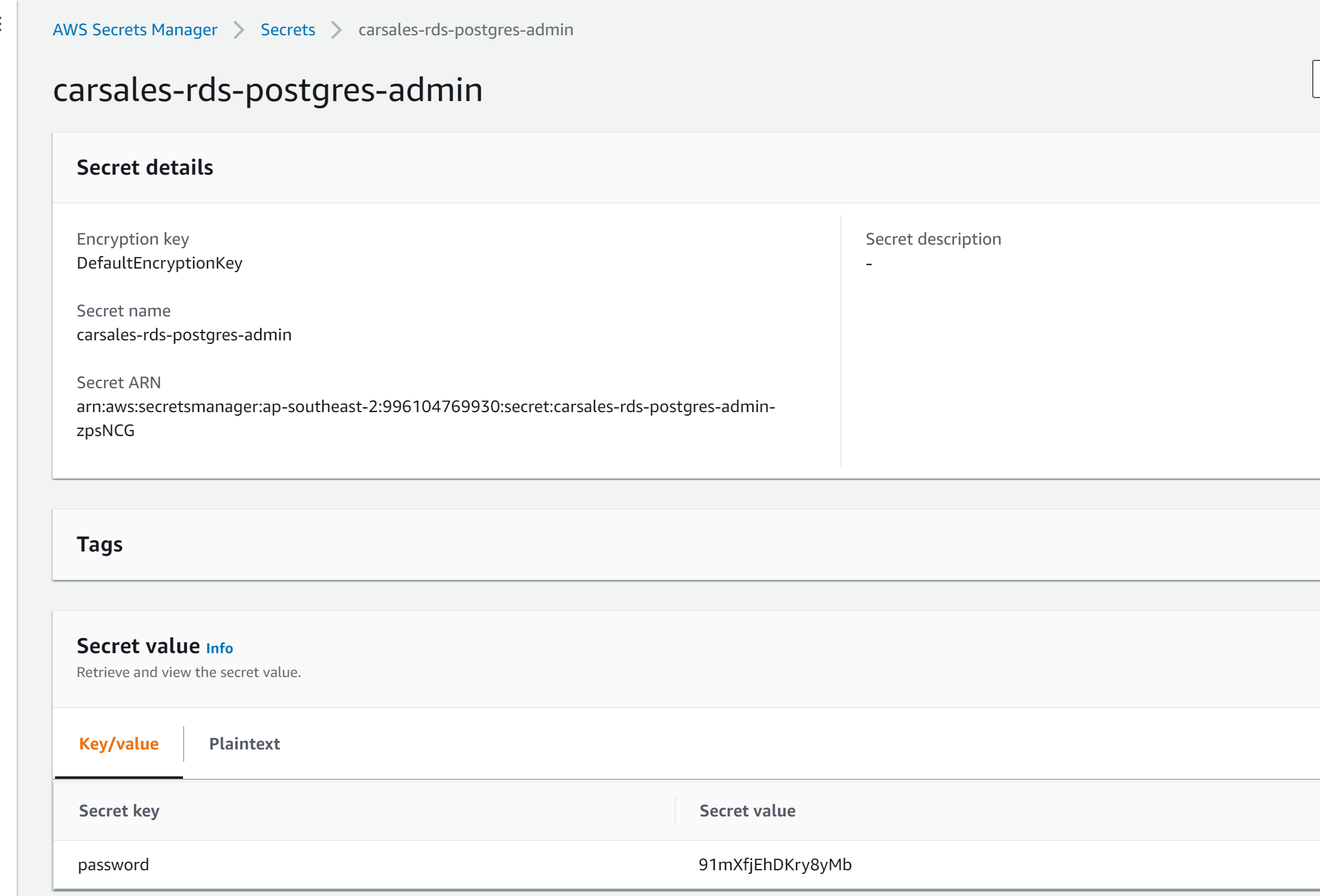
* EC2 instances which compose ECS clusters auto scale based on workload



* RDS db URL save to SSM parameter store.



* RDS Password is generated by random string is stored in AWS Secret Manager



* For secure reason RDS Security group only allow accessed from EC2 ECS instances.

