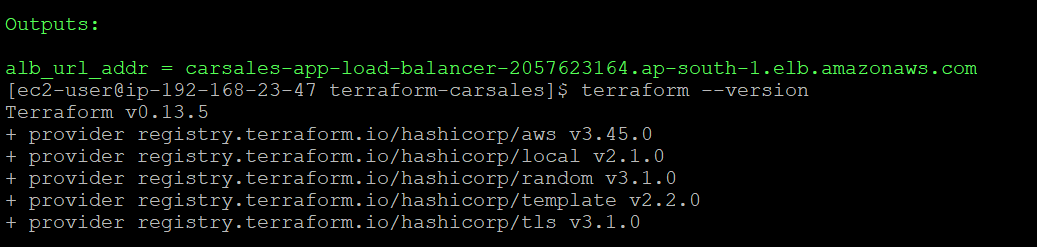
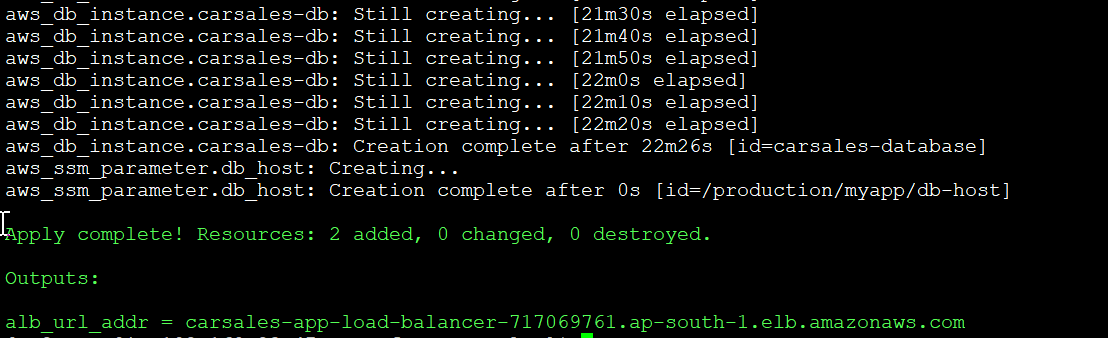
I used following terraform version



Terraform will output ALB URL (Since we will create RDS DB, it will took about 20 minutes to finish, just be patient)

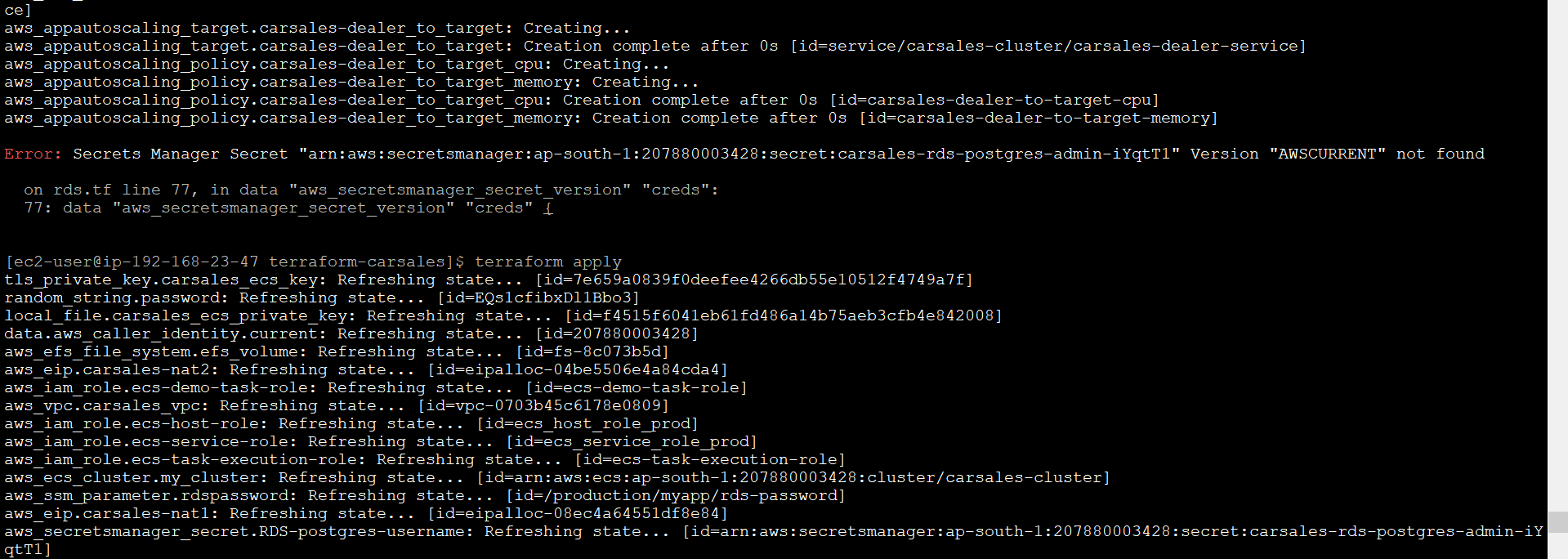


One potential bug met (chance of met it less than 20%)

Same symptom as <https://stackoverflow.com/questions/64016598/receiving-error-in-aws-secrets-manager-awscli-for-version-awscurrent-not-foun>

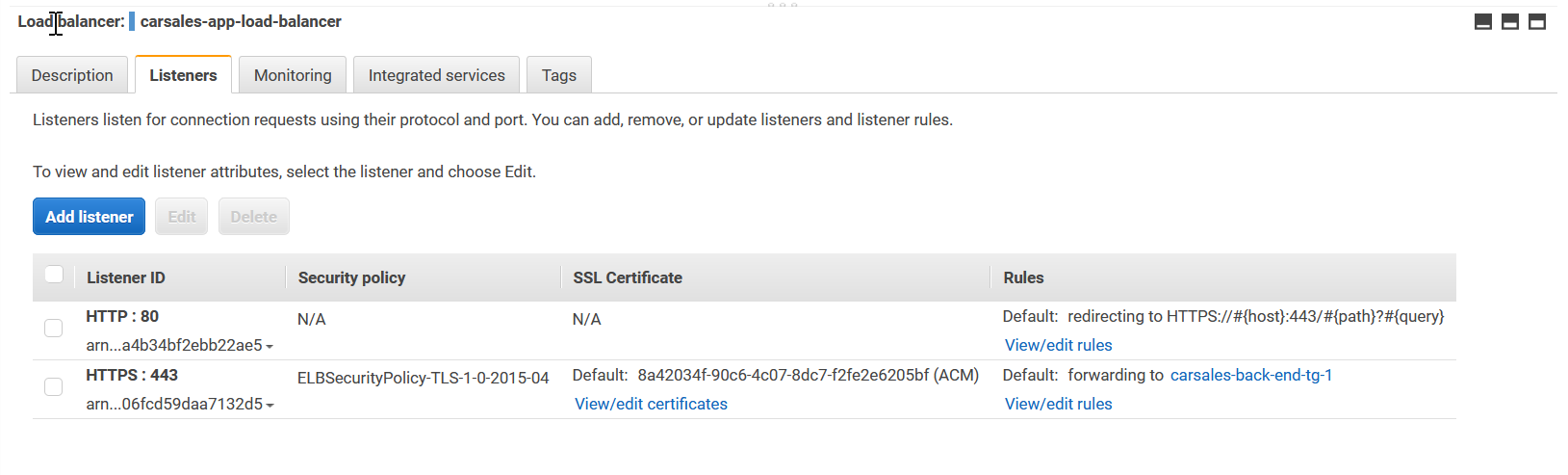
The AWS secret already created, but

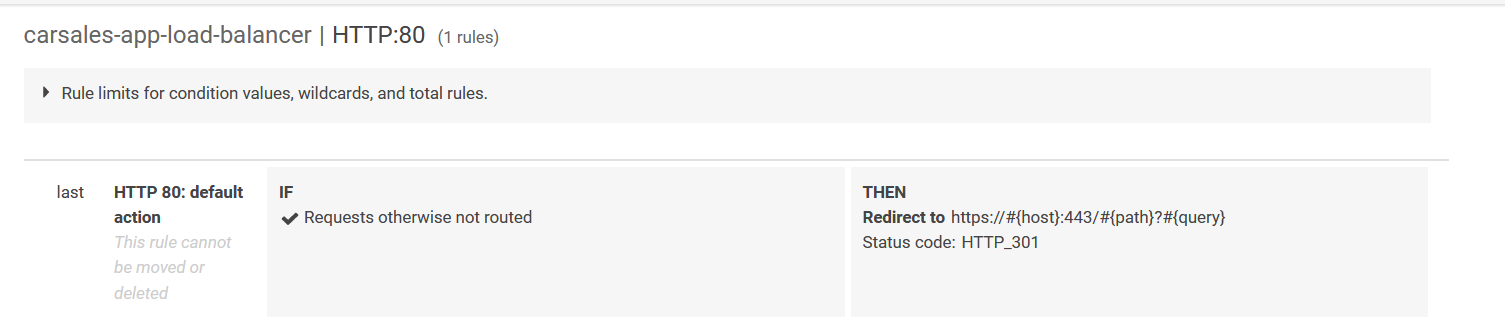
When met this issue, just retype terraform apply, everything is good.

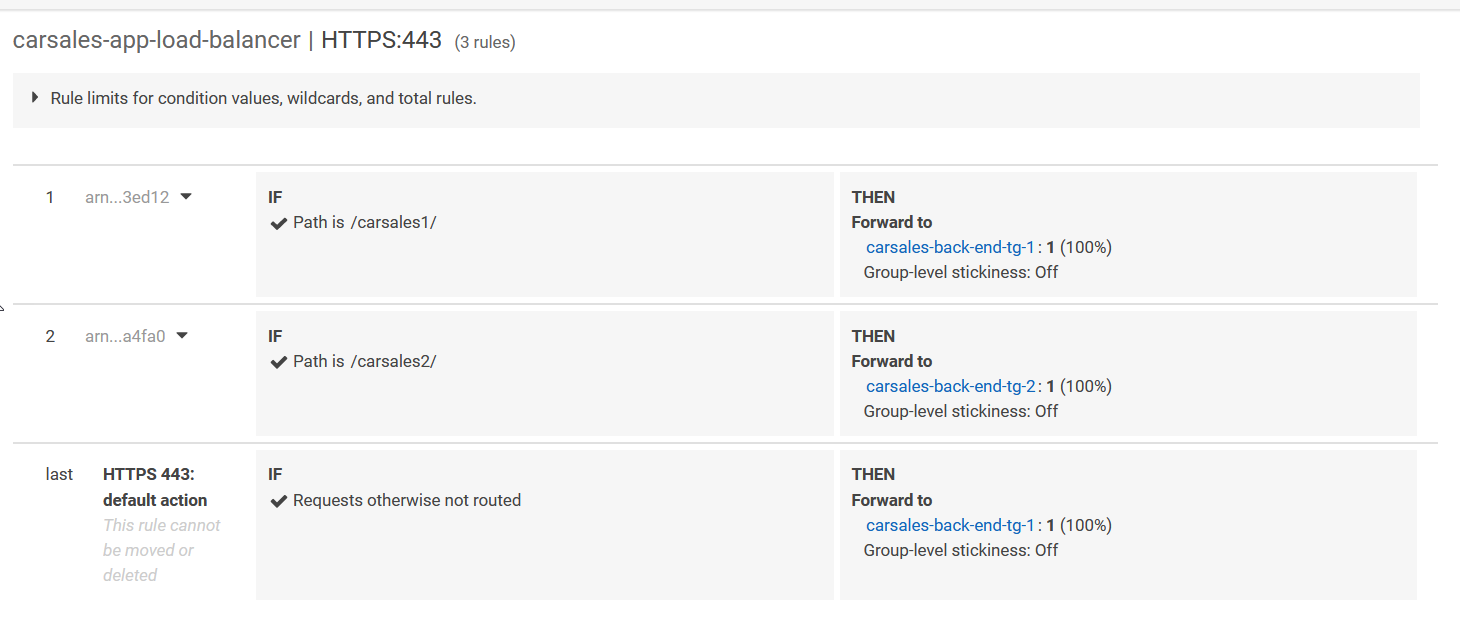


**Following features are only on my local test environment, since it need AWS Certificate Manager and Route 53 changes. The code I submit to you do not have this feature.**

**http to https redirect** when you input <http://carsales-app-load-balancer-685341695.ap-south-1.elb.amazonaws.com> it will automatically redirect to <https://carsales-app-load-balancer-685341695.ap-south-1.elb.amazonaws.com>



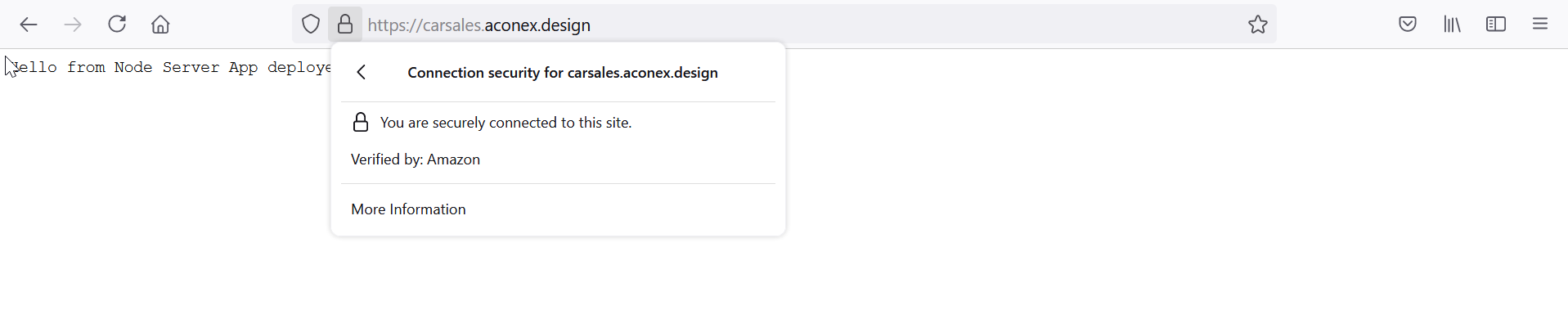




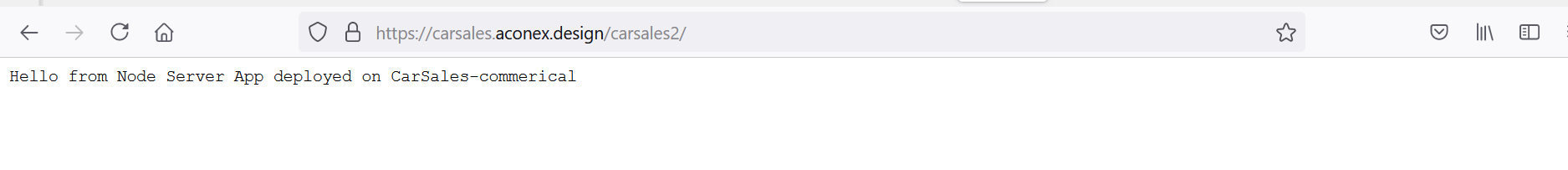
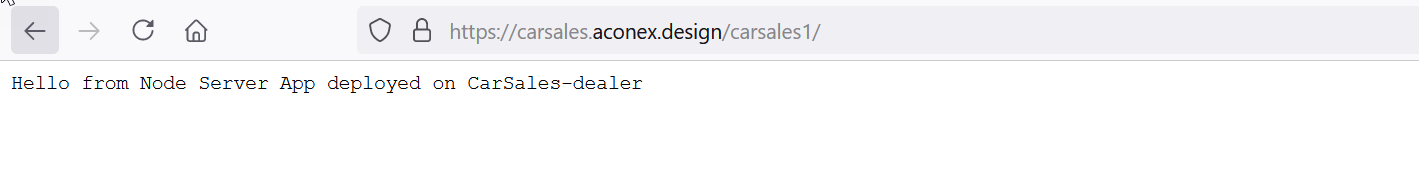
* Register ALB use Route53. Create carsales.aconex.design A record to ALB

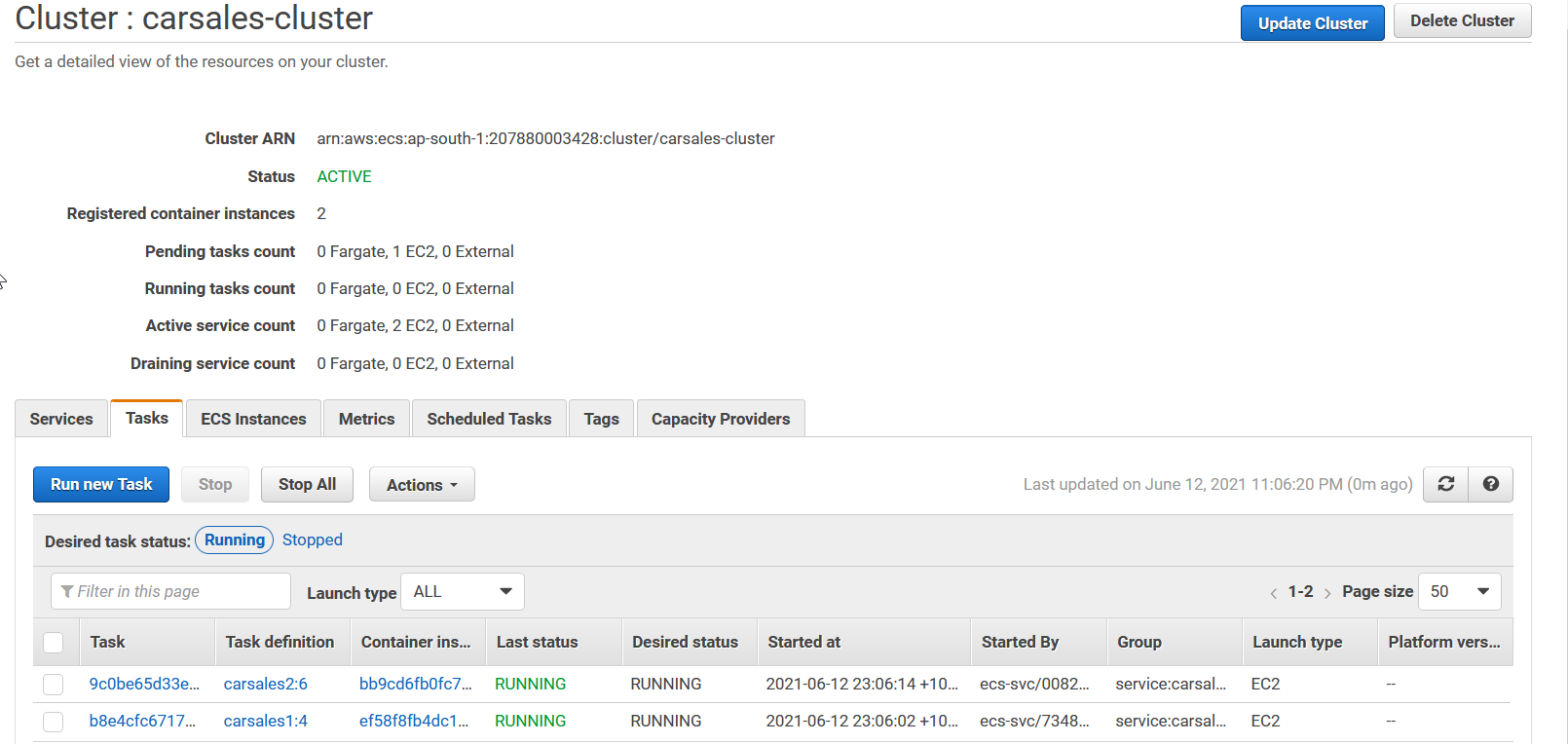


* Use Certificate get from AWS Certificate Manager (input https://carsales.aconex.design)

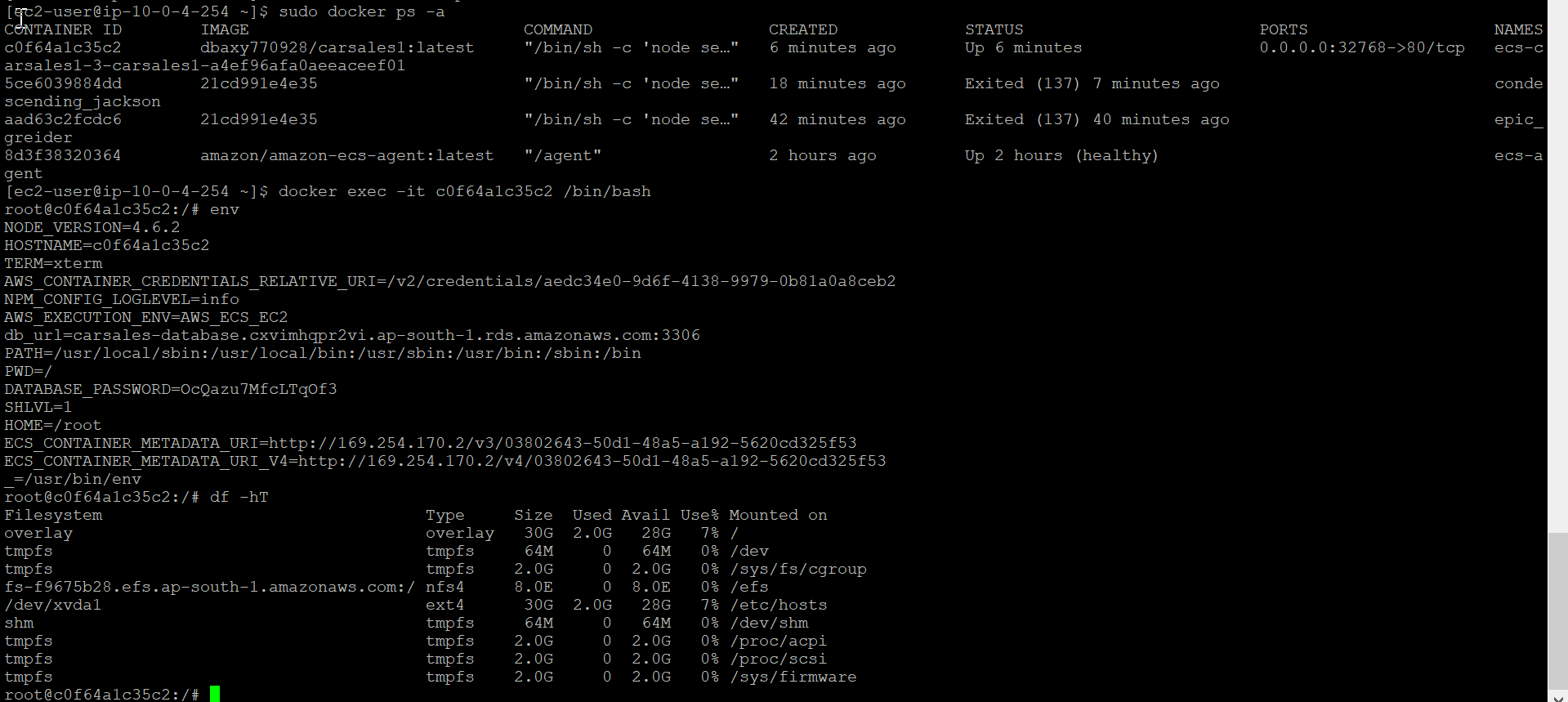


* ALB path based routing, different path related to different target group/ECS service

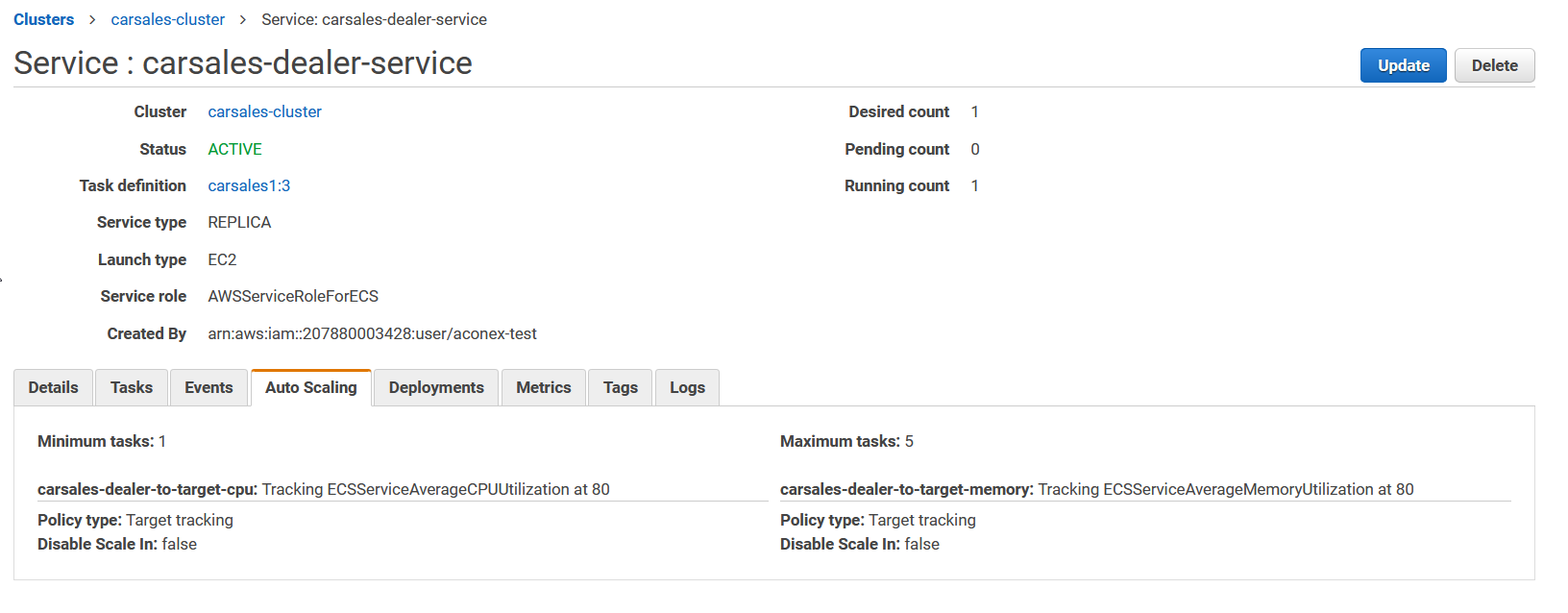




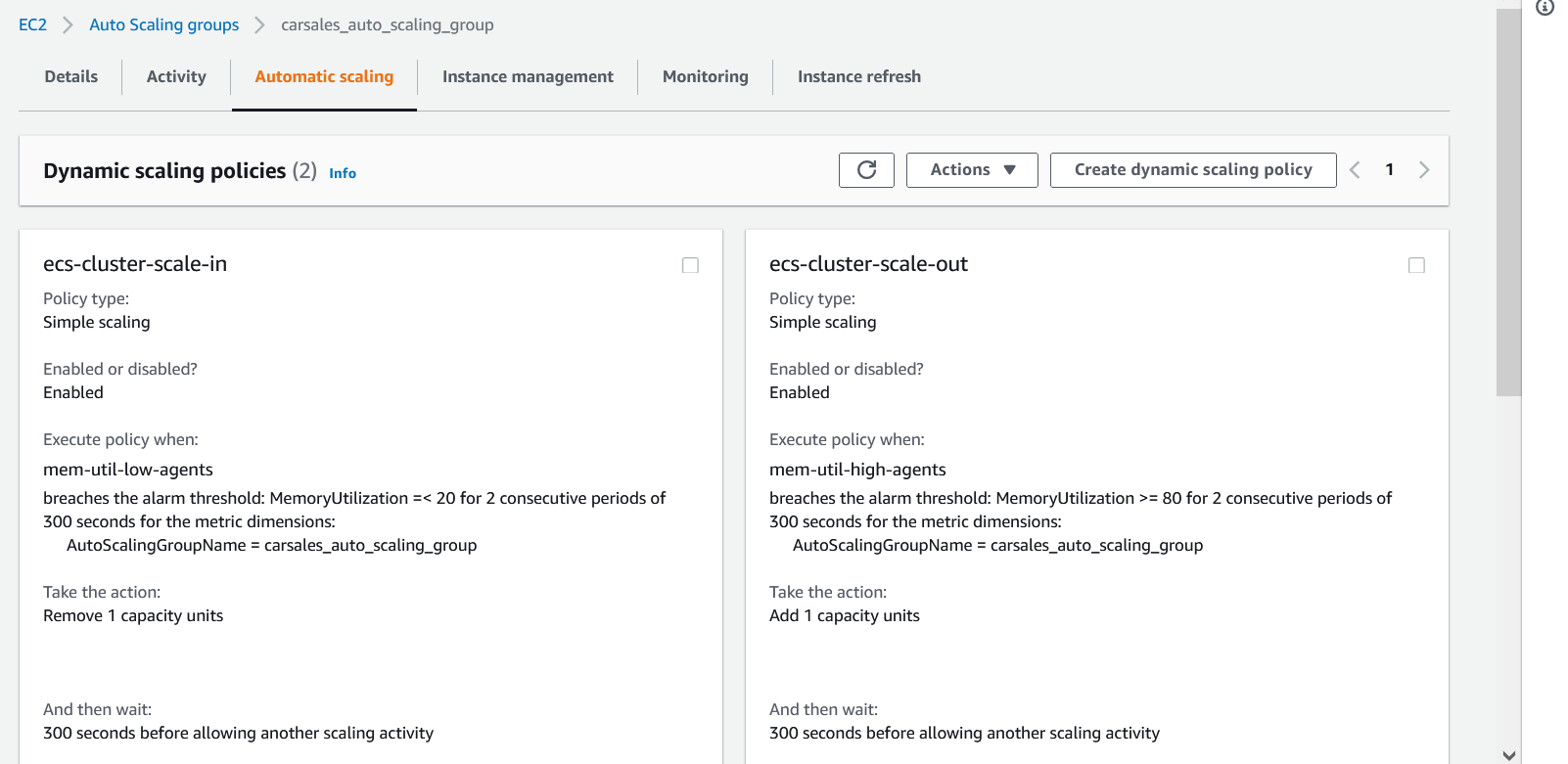
Access ECS EC2 instance from bastion host. Login to container and check command env output (you can find RDS db\_url and RDS database password which can be used to access database from docker container if application needed ) and df -hT (EFS mount) to store data outside in case docker container scale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



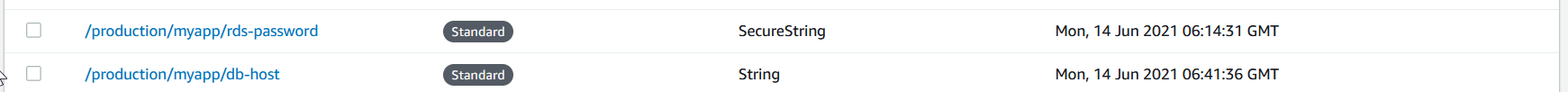
* ECS service autoscale based on load



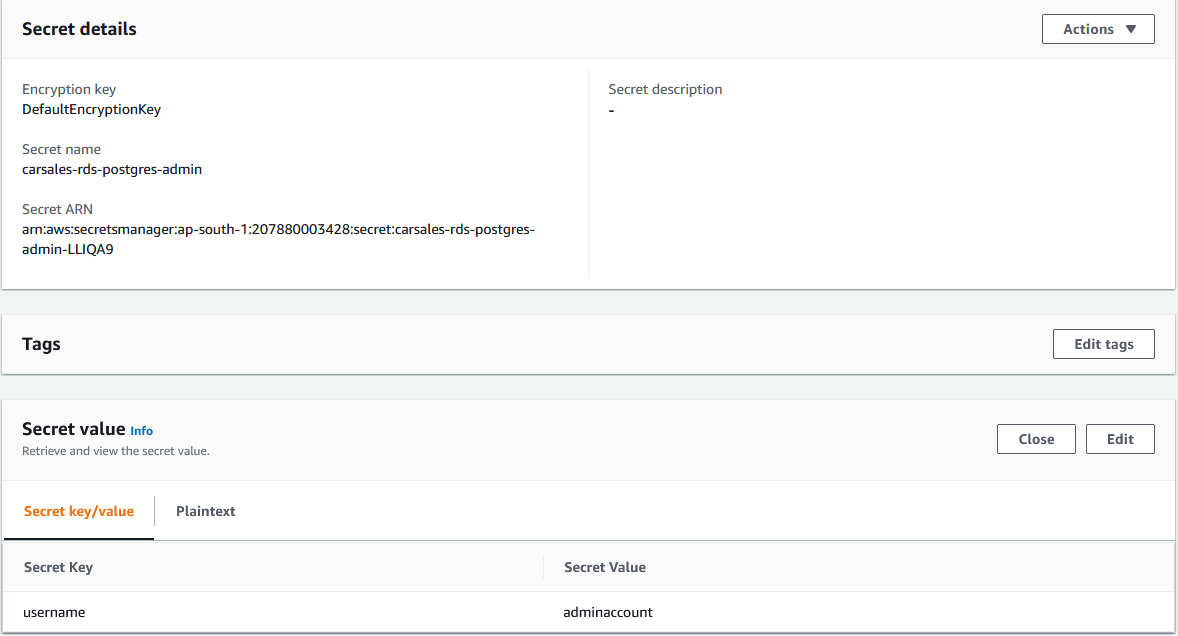
* EC2 instances which compose ECS clusters auto scale based on workload



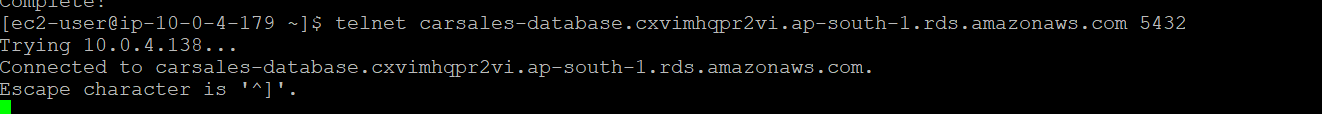
* RDS db URL and password save to SSM parameter store. Password is generated by random string.



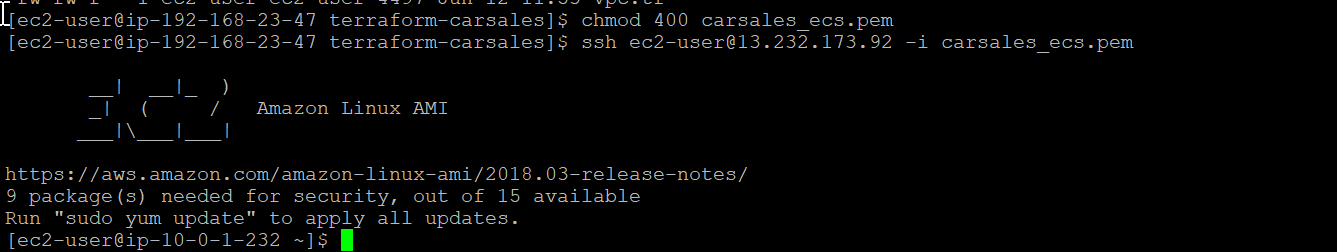
* RDS postgres username is stored in AWS Secret Manager



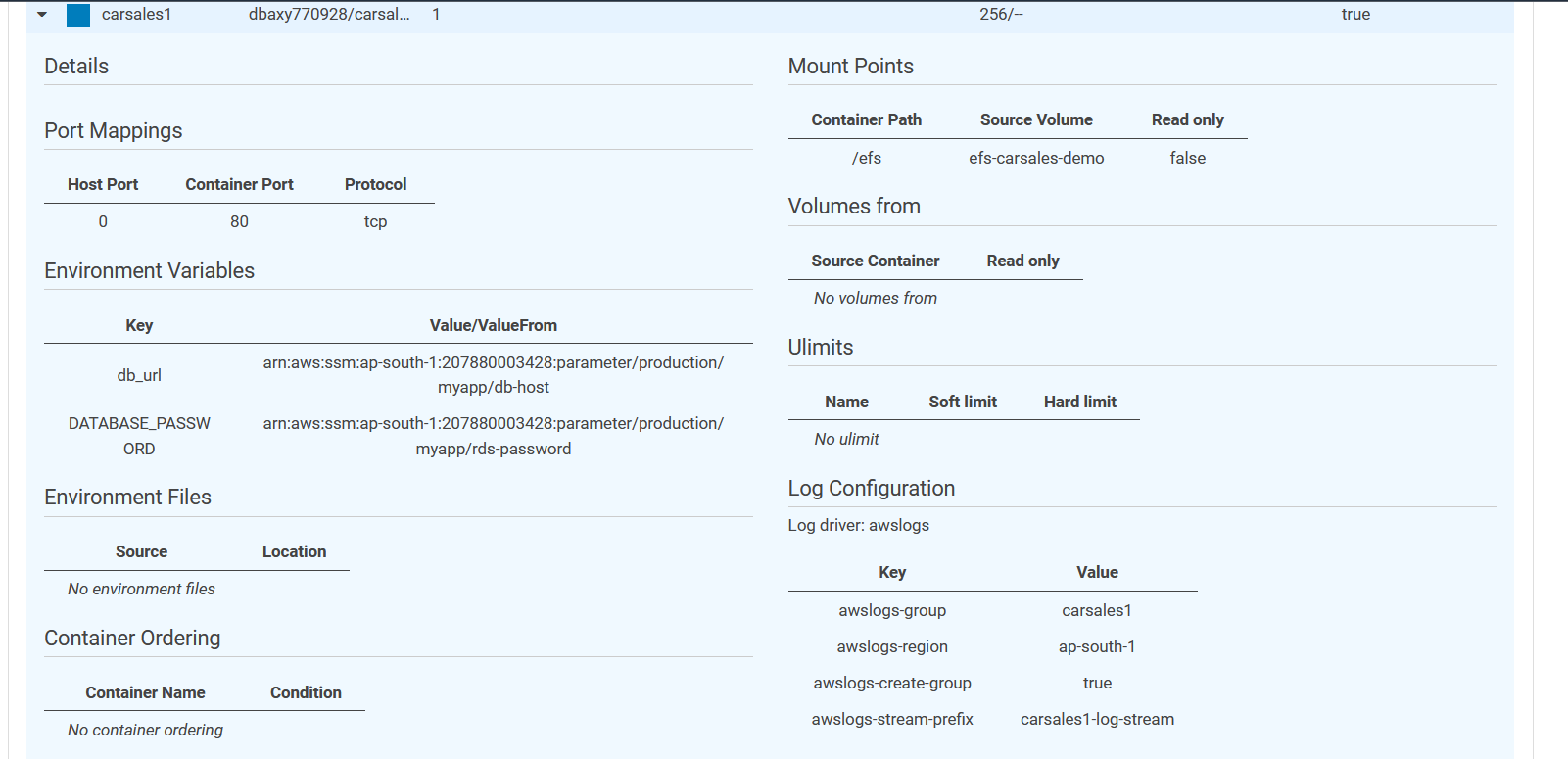
* For secure reason RDS Security group only allow accessed from EC2 ECS instances.

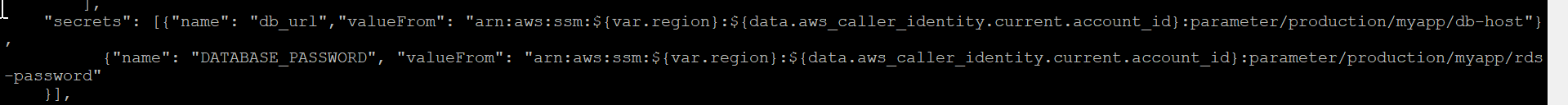


* Use generated key pairs to access bastion host and EC2 ECS instances (make sure chmod 400 the private key)



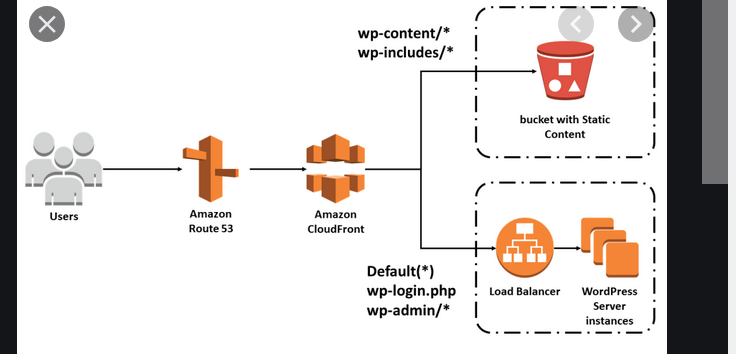
* Container definition will use aws\_caller\_identity to get account id related SSM parameter store

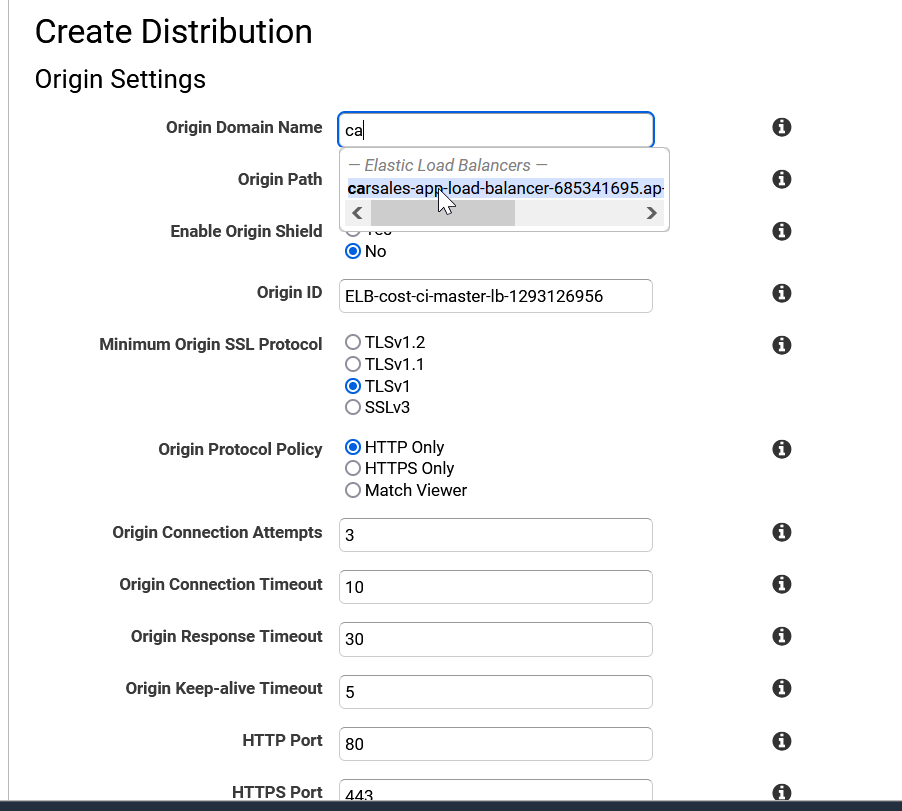


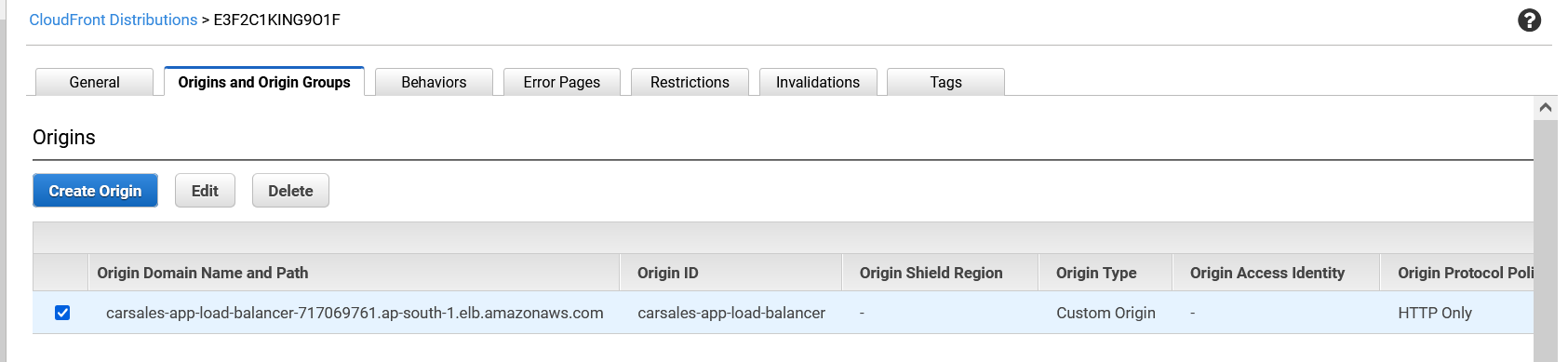


**Add on features (not in Terraform code)**

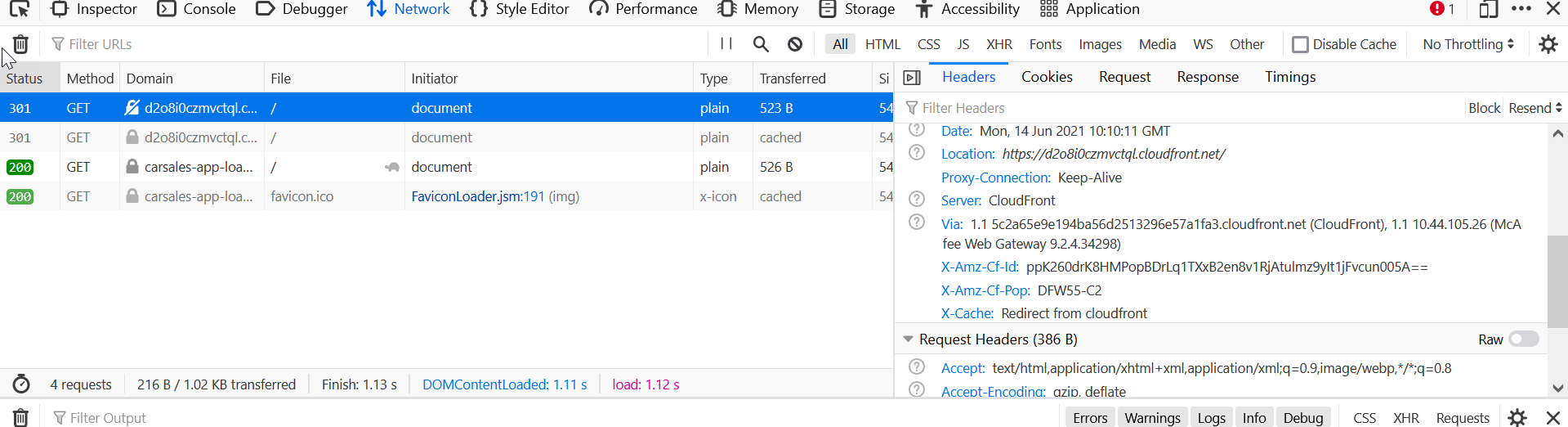
1 Create Cloudfront and set ALB is origin, if we hosts lots of static pictures and unchanged videos, user access contents cached at edge location.







When user input <http://d2o8i0czmvctql.cloudfront.net> will direct to ALB. Please check firefox debug screen please check it is cached



2 Direct Cloudwatch logs to ElasticSearch for analyze.

Notes

Those lines comment out because I do not have carsales certificate information. In my local environment, I have certificate get from AWS ACM. So in my environment, I have https and http redirect to https, you will only accept http with no encryption.

