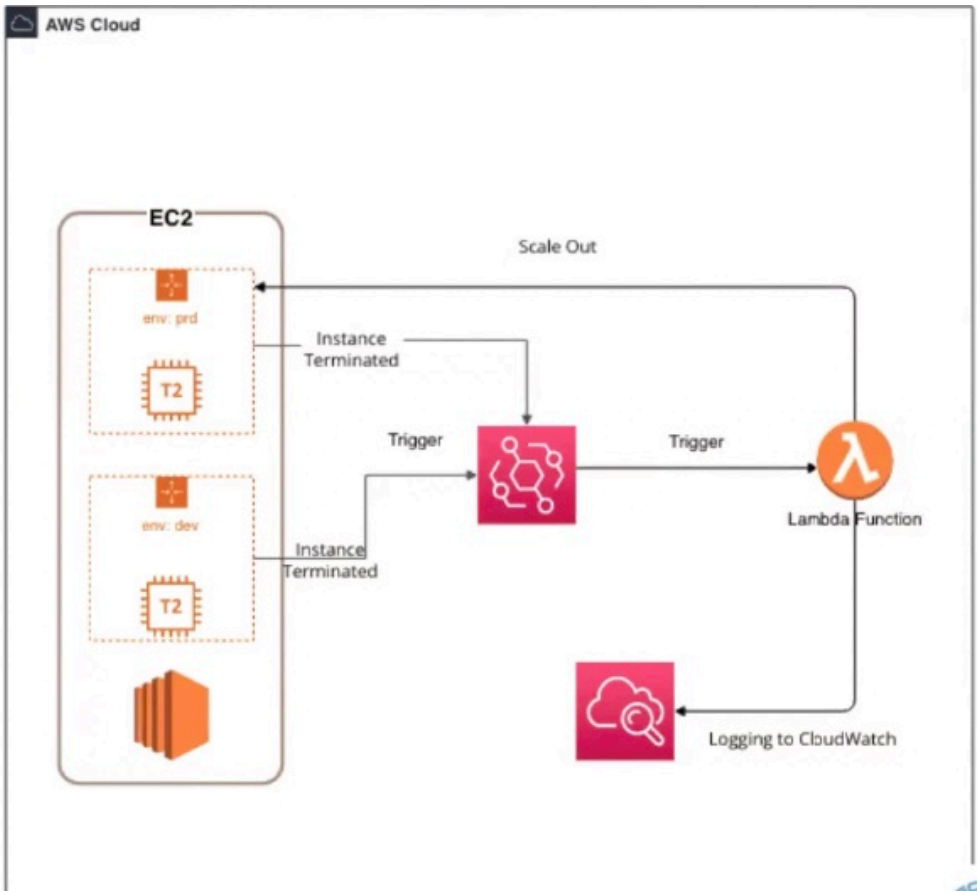
Mini Projects

Auto Remediation

A company uses a ‘multiple environment to a single AWS account’ approach for EC2 deployments. The manager has noticed that there have been outages due to junior engineers accidentally changing desired capacity of the production ASG to 0. IAM permissions are avoided for now and you are asked to put an auto remediation solution to auto recover from these mistakes.

Solution



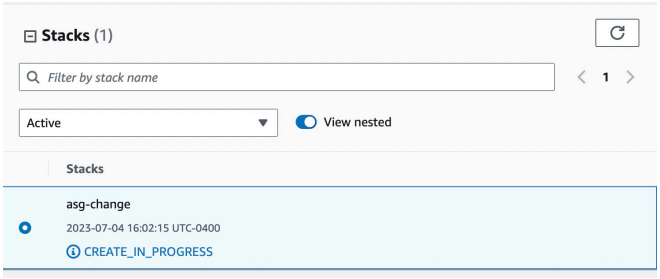
When Auto Scaling group desire is dropped, it should trigger a function and this should return and improve autoscaling.

In Event Bridge, instance terminated events are sent to the the Lambda function when the event bridge is triggered. Lambda is also looking at whoever this event came from.

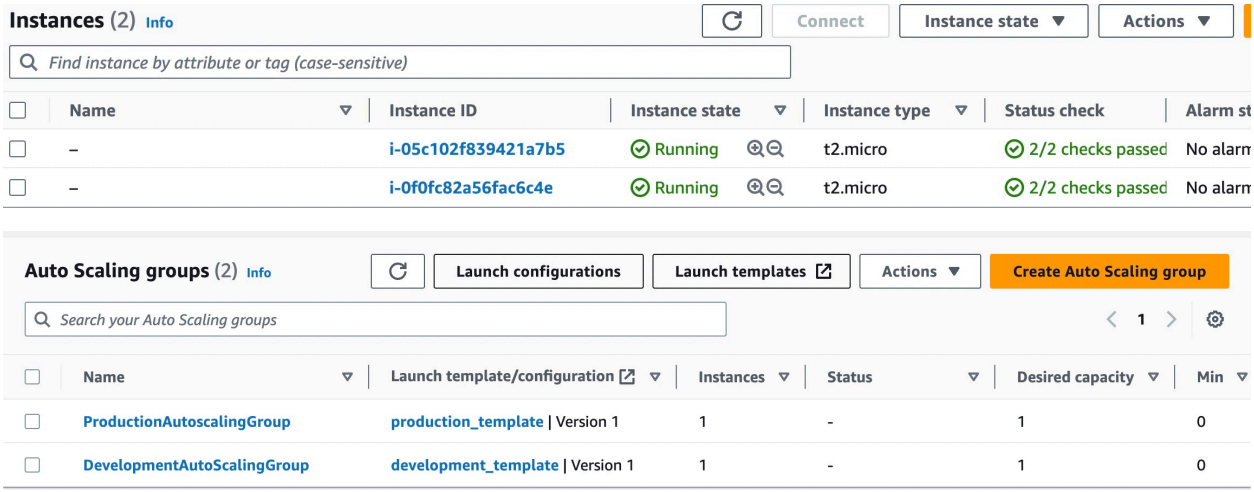
It doesn’t matter if it came from dev, just directly write it to Cloudwatch. If the event came from production, Lambda edits autoscale and redirects it to EC2 and rearranges auto scaling. You can enter the id number of EC2 in the services in Eventbridge.
Target 1 is aws service lambda function, selected function name is asg-change.

Part 1

I created a stack on CloudFormation. I uploaded a template file on Specify Template. Stack name is “asg-change” tag key ‘app’ , value is ‘asg-change’.

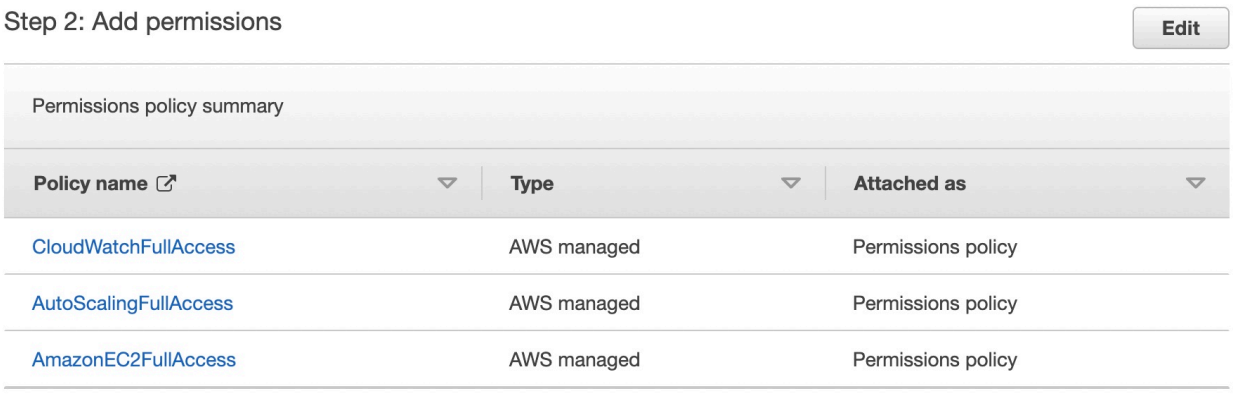


Cloudformation started 2 instance machine and 2 autoscaling group.



Part 2

I created IAM role. I selected Lambda. In order, I choose EC2FullAccess, CloudwatchFullAccess, AutoScalingFullAccess. Role named ‘asg-change-lambda_role’

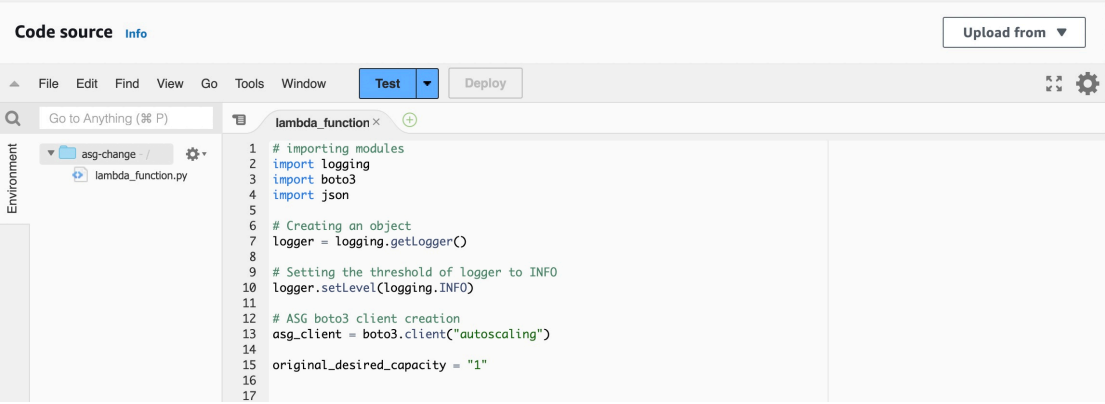


Part 3

I created a function on Lambda. I selected author from scratch, named ‘asg-change’, runtime Python 3.9.
Under the “Change default execution role”, use an existing role I choose the asg-change-lambda_role I already created. I pasted the code is given for Lambda function.

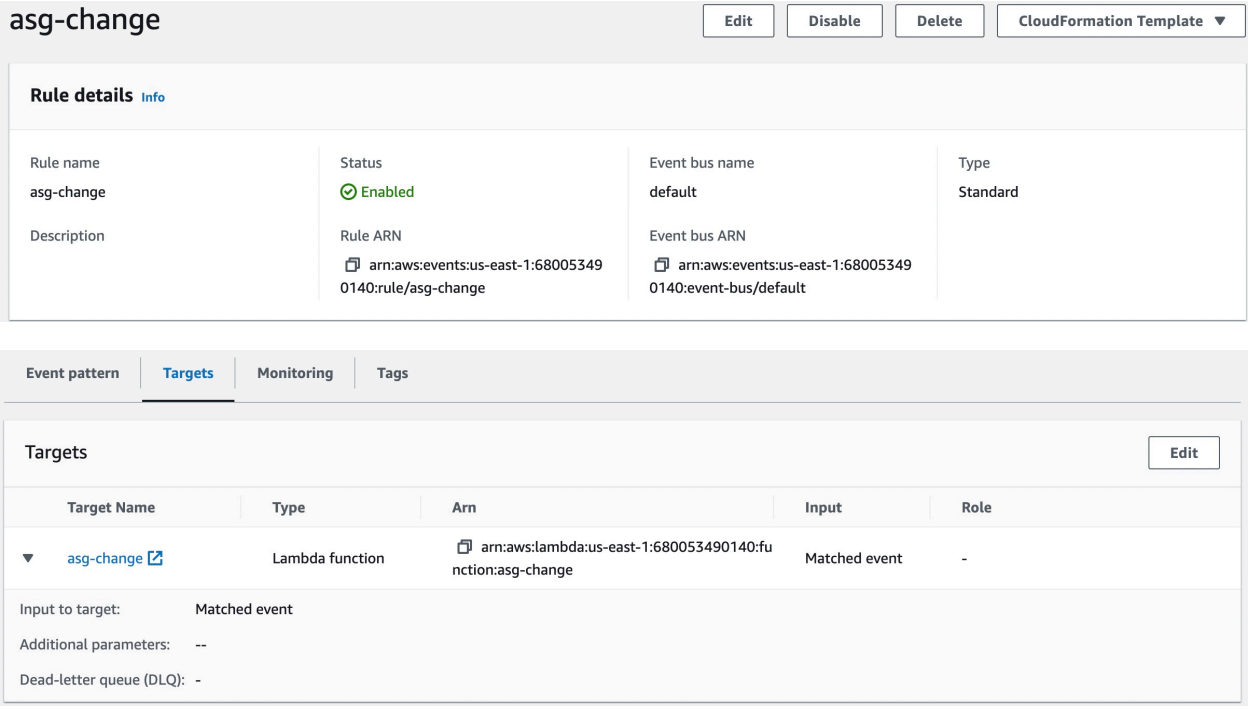
This code lets Lambda to edit autoscale and redirect it to EC2 and rearrange auto scaling.

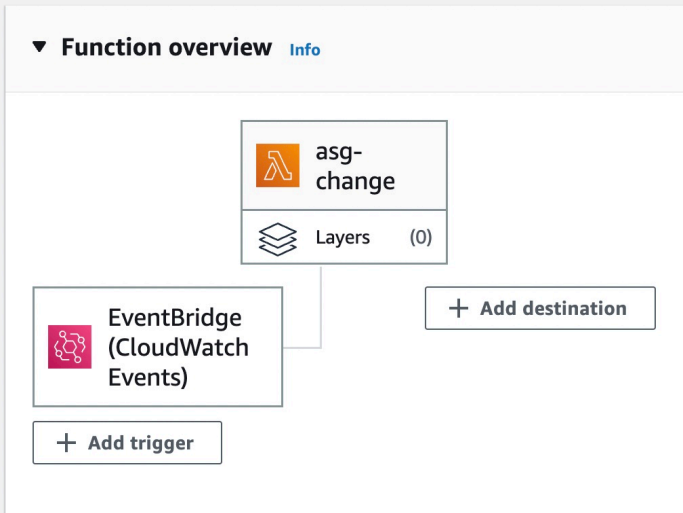
I click on “DEPLOY”



Part 4

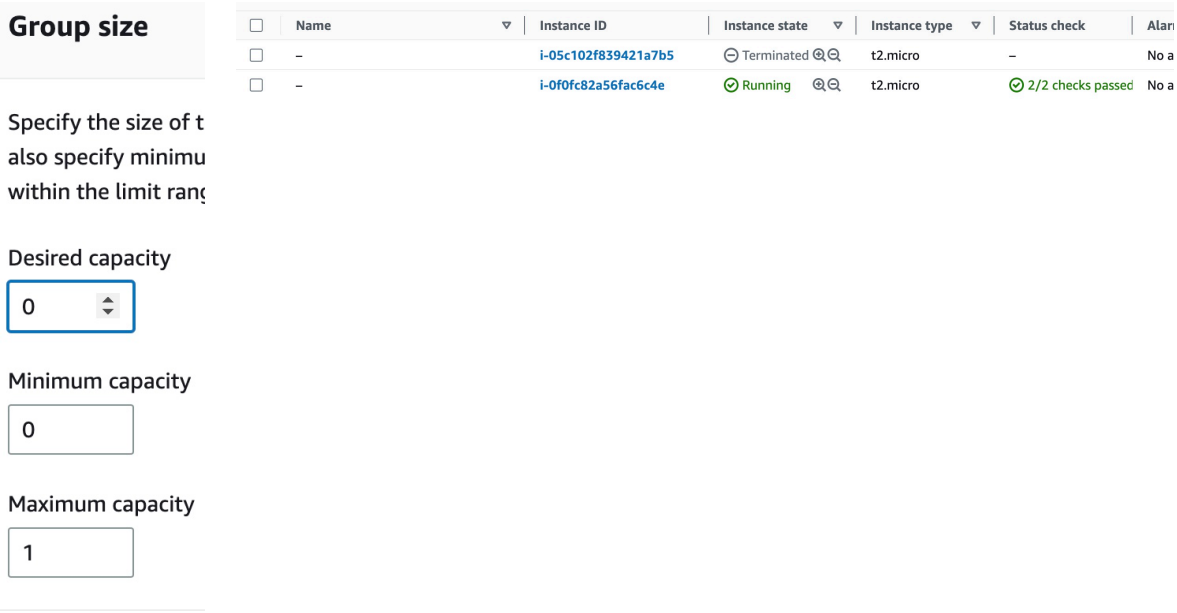
I created a rule on Eventbridge. Rule name is ‘asg-change’, event bus default. Event source AWS events or Eventbridge partner events, sample events is ‘EC2 Instance Terminate Successful’
Event Pattern, AWS service is AutoScaling, event type Instance launch and terminate.





Part 5

I edit development autoscaling group like junior engineer did. I changed desired group to 0. An instance had terminated.



This time, I edit production autoscaling group. I changed desired group to 0. In the cloudwatch log says desired capacity changed to 1. And another instance had initiated. Production desired capacity had changed to 1. Because Lambda took the message from Eventbridge