AWS SOLUTION ARCHITECT

Client service report

Author
Niall CREECH

October 8, 2019

Contents

1 Solution analysis

The current implementation cannot be accessed from external networks. The service consists of,

- Networking is a VPC with CIDR 10.0.0.0/16 with 2 public subnets 10.0.0.0/24 and 10.0.1.0/24 in eu-west-1b and eu-west-1b respectively, as well as 2 private subnets 10.0.2.0/24, 10.0.3.0/24 in eu-west-1b and eu-west-1b.
- VPC has an internet gateway and a classic load balancer (ELB)
- Routing is setup up to allow all traffic between subnets and out to external addresses.
- There are 2 security groups, one for the single EC2 application instance, and one for the ELB.
- DNS is enabled and the instance has a pubic IP address

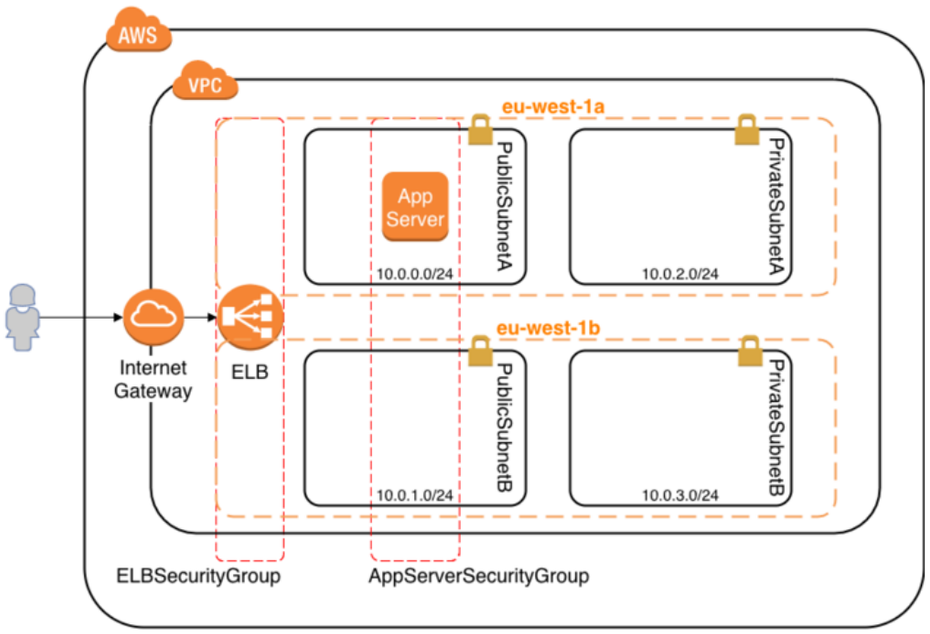

Figure 1: My explanation

1.1 ELB healthcheck on wrong instance port

Summary: Httpd starts on-instance on port 80. The ELB correctly forwards ports from from 80 to instance port 80. However, the healthcheck looks to verify instance health on port 443 through a tcp connection. This change simply targets the healthcheck correctly at port 80 on the instance.

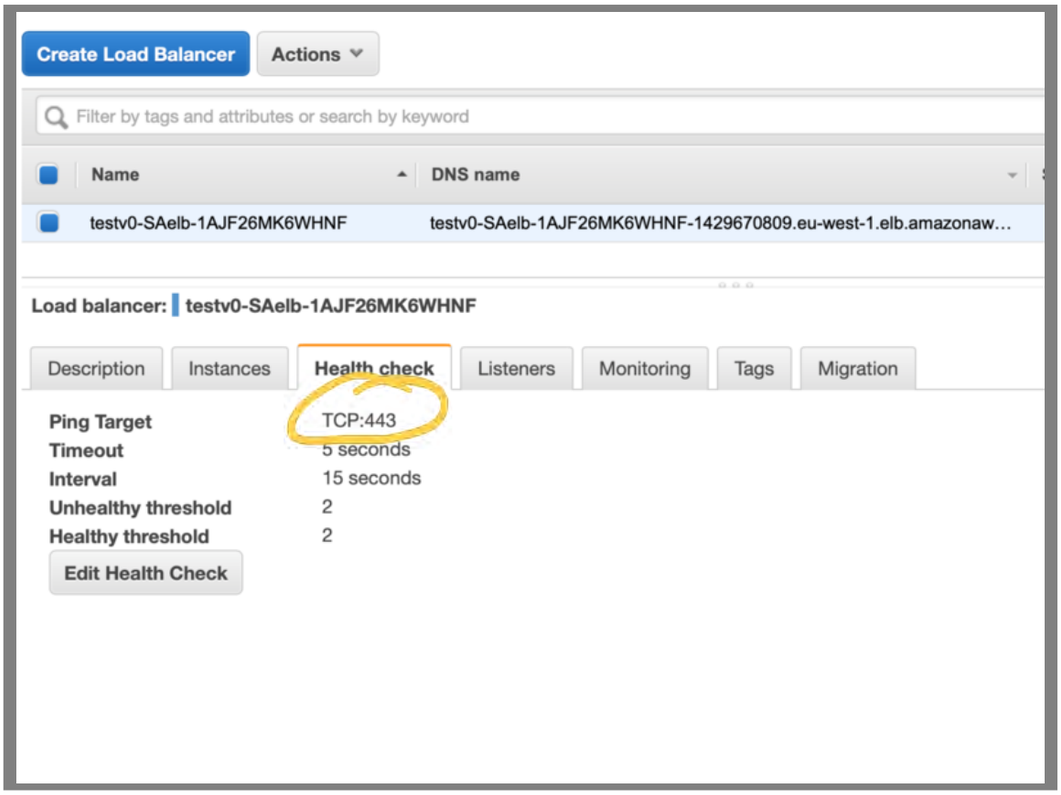

Figure 2: In the AWS console, navigate to Services → EC2 → Load Balancers and select the 'Health check' tab.

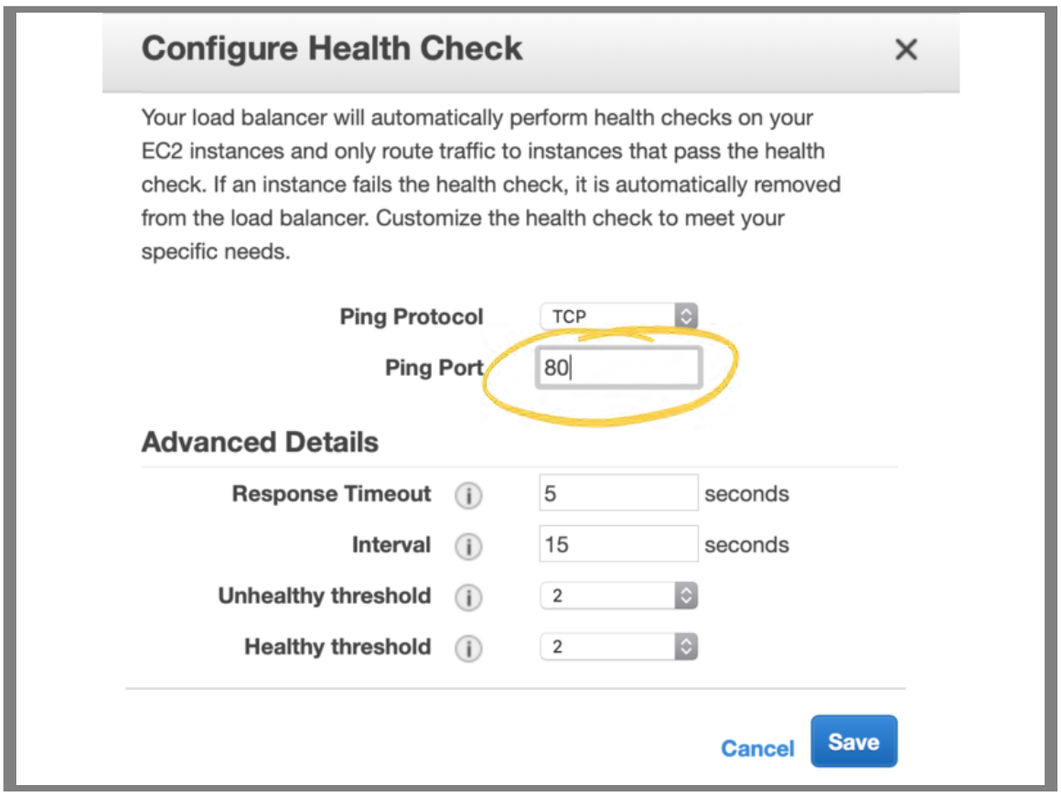

Figure 3: Change the port from 443 to 80. This will leave the load balancer checking the instance health by connecting through tcp on the servers default HTTP port.

1.2 Load balancer cannot route to subnet

Summary: The ELB can only route to instances in PublicSubnetB. This change allows it to route to PublicSubnetA also, where the current instance is located.

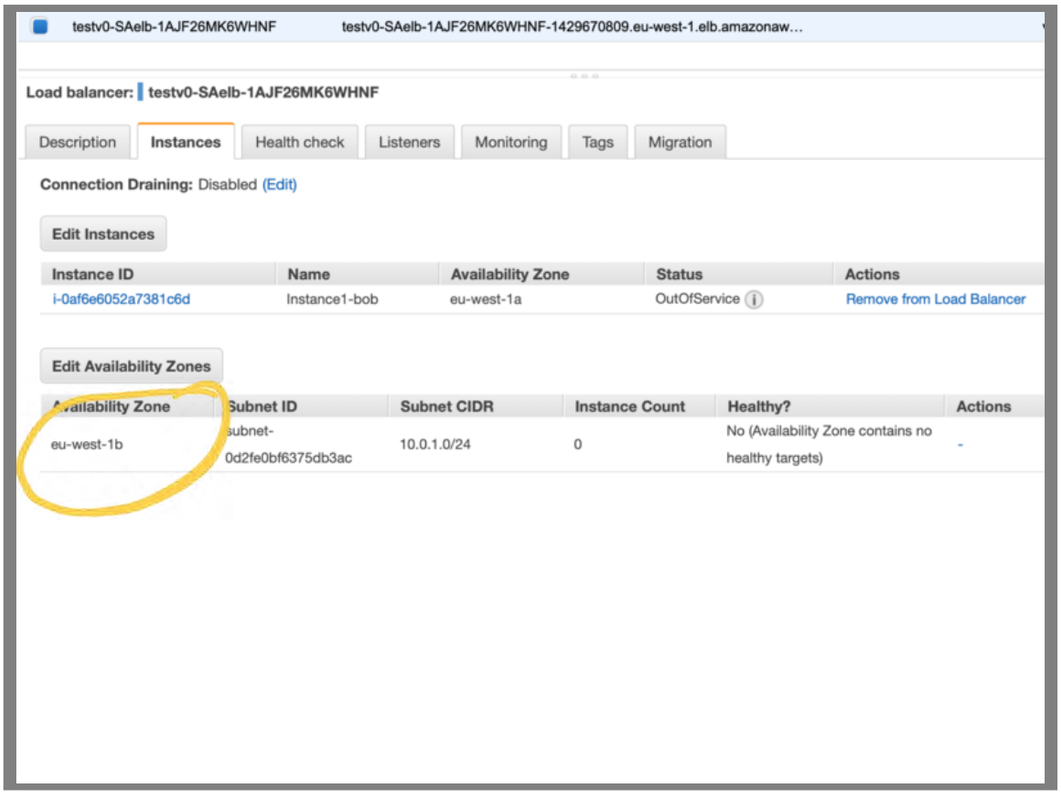

Figure 4: In the Load Balancers configuration page, select the load balancer and then the 'Instances' tab. Note that only the eu-west-1b zone is available to the load balancer, which has no instances

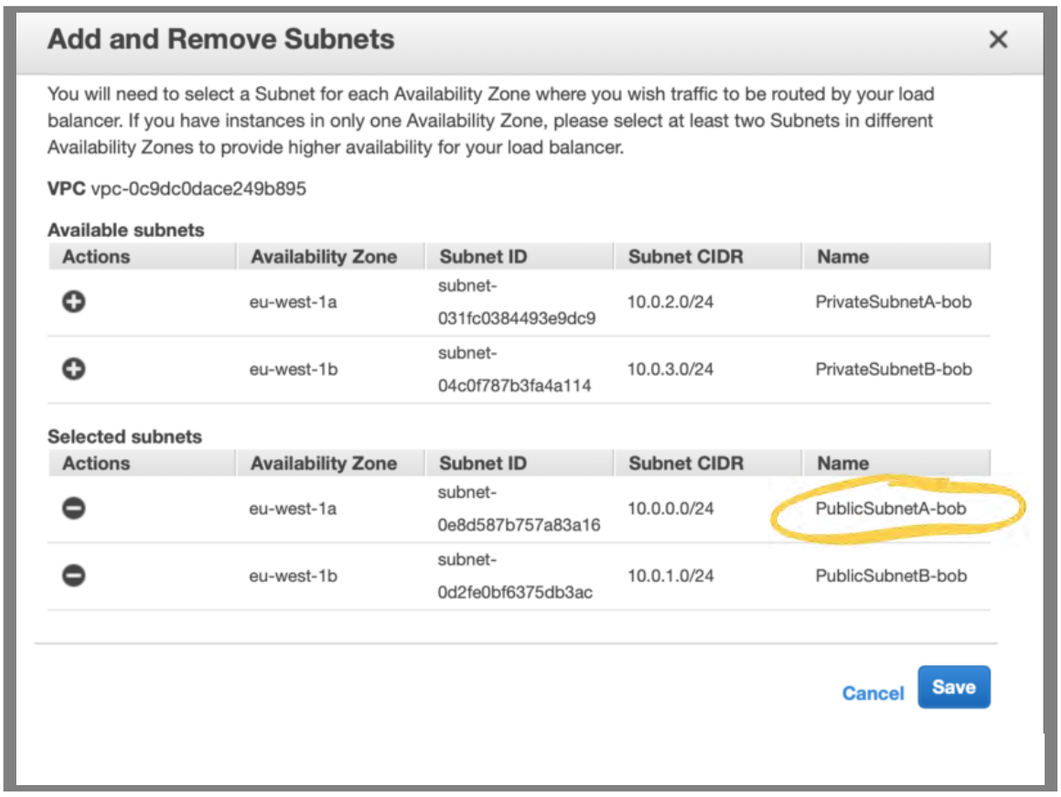

Figure 5: Add 'PublicSubnetA' to the load balancers available subnets. This means that the load balancer can now direct traffic to the instance in eu-west-1a

1.3 The site cannot be accessed from external addresses

Summary: Allow all addresses to access the load balancer on port 80

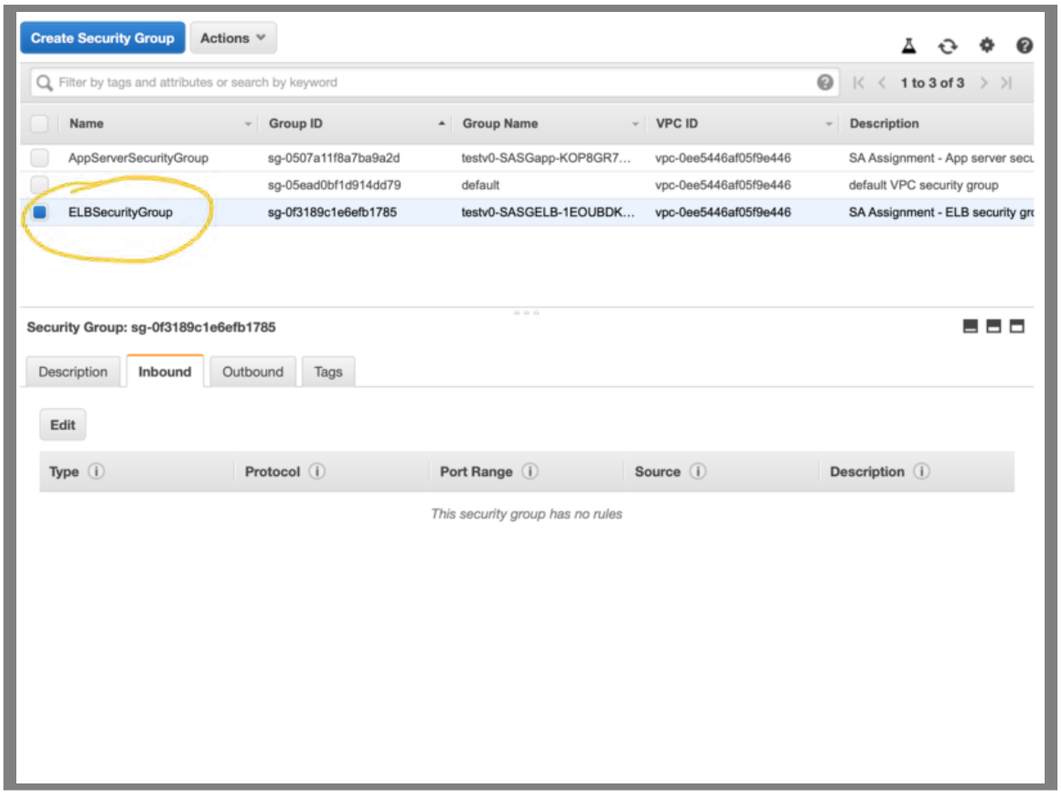

Figure 6: Navigate to Services → EC2 → Security Groups. Select the ELBSecurityGroup group and the 'Inbound' tab. By default, no inbound rules are set.

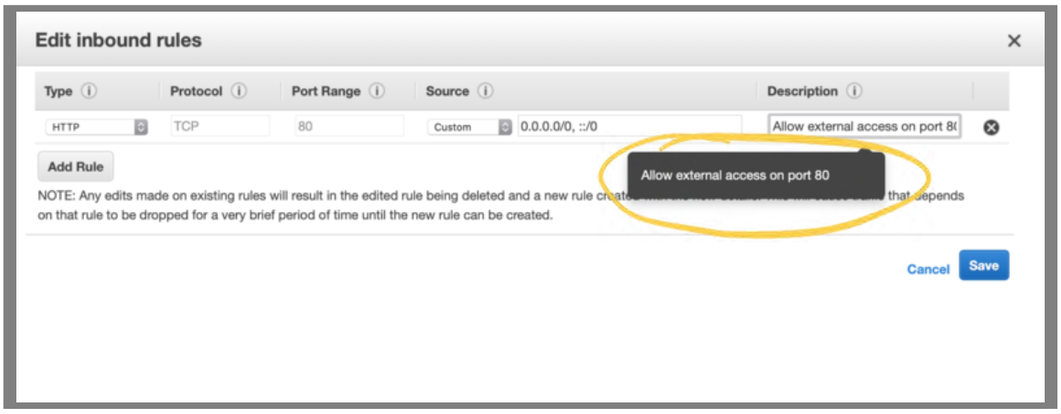

Figure 7: Edit the group and add an inbound rule to allow http access from everywhere, 0.0.0.0/0. Users will now be able to reach the load balancer from the internet and other external networks.

1.4 Instances cannot be accessed from the load balancer

Summary: This change allows traffic from the ELB to the instances. This is set to all TCP traffic to port 80 to allow the ELBs TCP-based healthcheck to pass

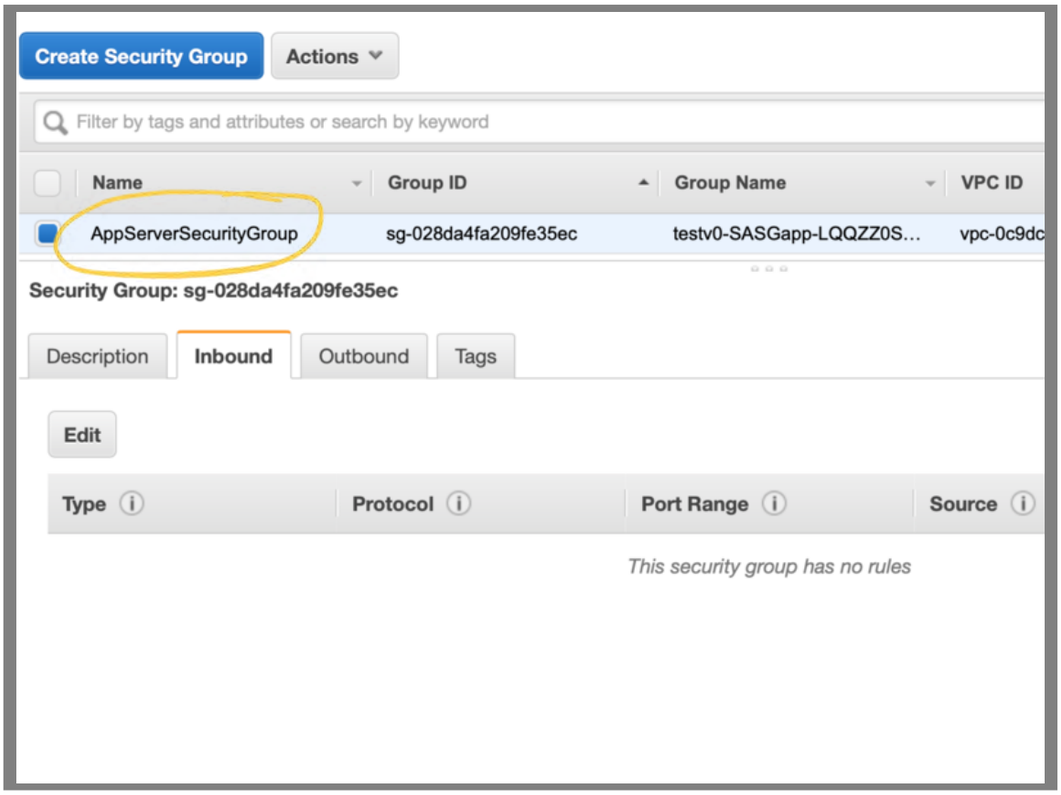

Figure 8: Still in the 'Security Groups' section, select the 'AppServerSecurityGroup' group and the 'Inbound' tab. As we can see, there are no rules set.

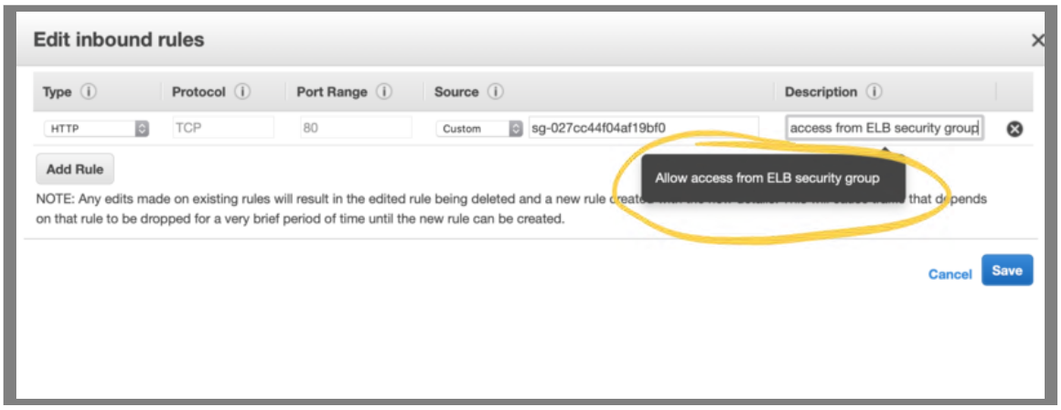

Figure 9: Edit the group and add an inbound rule to allow http access from the ELBSecurityGroup. The security group Id needed for the 'Source' value can be found by typing 'sg' then choosing from one of the values in the popup menu.

1.5 Success!

You should see the site on your loadbalancers domain name `http://<load-balancer-dns-name>/demo.html`. The right DNS name can be found on the 'Description' tab of the 'Load balancers' configuration page when your load balancer is selected.

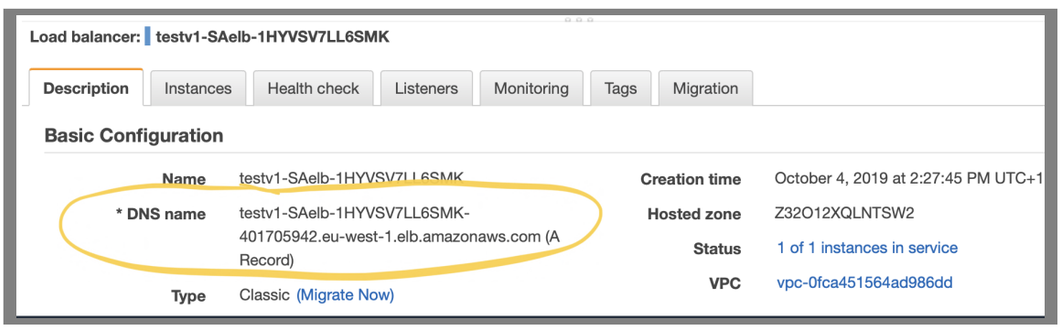

Figure 10: The DNS name of the load balancer can be found in the load balancers description tab

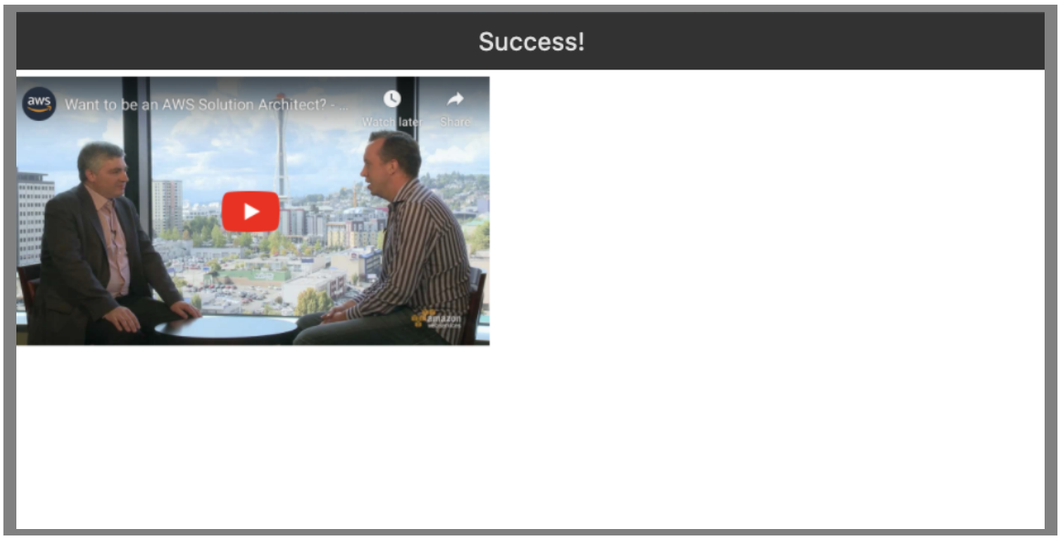

Figure 11: The instances are now reachable through the load-balancer to customers on the internet

2 Solution Enhancement

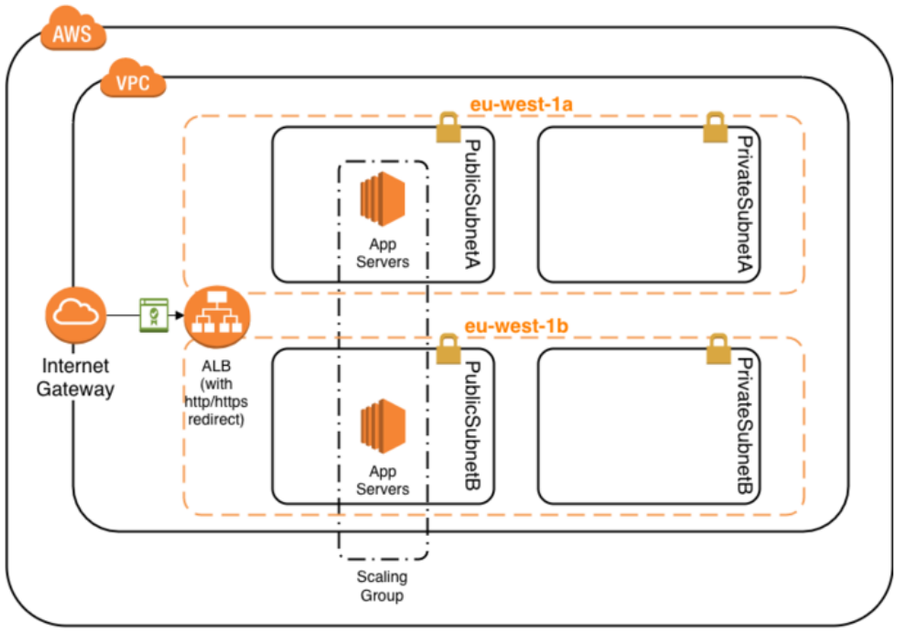

Figure 12: My explanation]

2.1 Operational

The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures

2.1.1 Improve monitoring and logging

Monitoring and logging on the existing instance can be increased by enabling the cloudwatch agent on the application instances

2.2 Security

The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies

2.2.1 Harden EC2 instances

2.2.2 Enable SSM session manager

2.2.3 Strengthen NACL to prevent cross-subnet traffic

2.2.4 Only allow NACL to pass traffic to private subnets from public subnets

The private NACL allows all external traffic to pass. We can increase security by allowing only access from public subnets, or additionally from private endpoints, NAT gateways etc.

2.3 Reliability

The ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues

Currently there is a single instance with no auto-recovery

2.3.1 Replicate instances into multiple AZs

2.3.2 Create an auto-scaling group for application instances

2.4 Performance

The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve

2.4.1 Change instance type

The current solution uses bursting t2.micro instances with CPU credit limits. This is very cost efficient, but performance is not suitable for reasonable traffic levels and exhausting CPU credits will cause degradation of availability.

2.5 Cost

The ability to run systems to deliver business value at the lowest price point

3 Future expansion

[?]

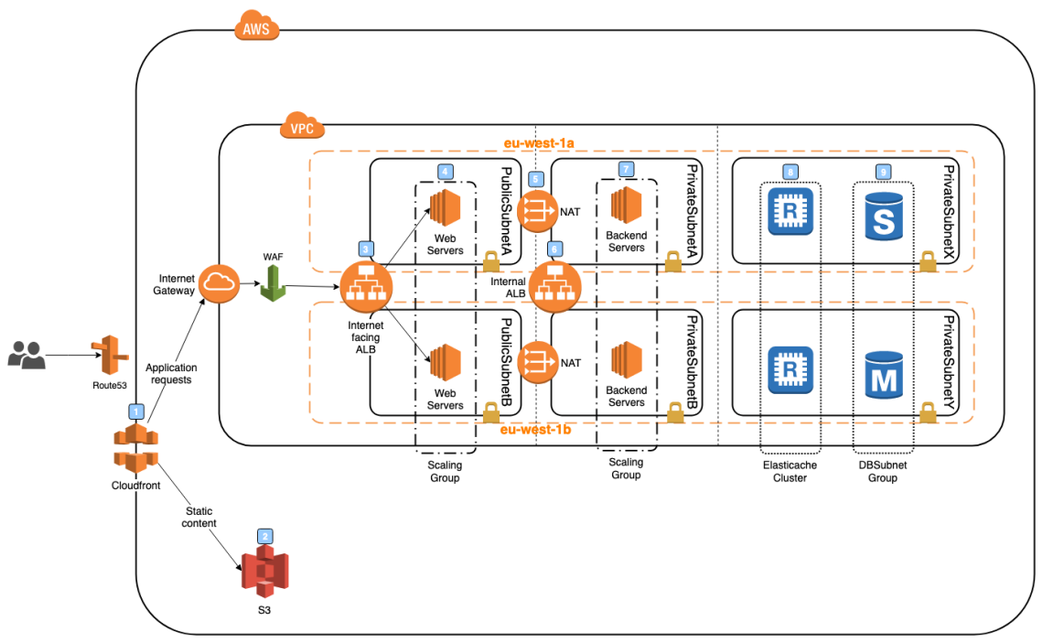

Figure 13: My explanation]

(1) Users get DNS resolution from Route53 entries
(2) Cloudfront provides cached content from edge locations around the world.
(3) A secured S3 bucket provides a highly scalable source of static content
(4) Active content is sourced through a public application load balancer (ALB).
(5) WAF is configured with rules in front of the ALB
(6) Applications requiring public internet addresses are installed on EC2 instances inside an auto-scaling group (ASG) in public subnets distributed across more than one availability zone.
(7) The NAT gateway service provides address translation to allow outbound internet access for the private subnets
(8) Applications that do not require public internet addresses are installed on EC2 instances inside an ASG in private subnets distributed across more than one availability zone.
(9) Elasticache (redis) provides in-memory caching for the database backend.
(10) RDS in multi-AZ mode gives resilient failover from primary to secondary, as well as < 5 min point in time recovery.

References