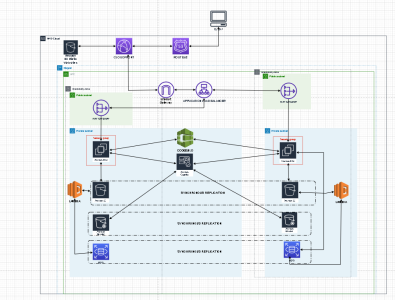
GeeGee — Today at 11:13 PM

[](https://cdn.discordapp.com/attachments/423842546947457026/930585322683768902/unknown.png)

Bards Aren't Real — Today at 11:15 PM

AZs look fine. 2 is the minimum you should be using and is perfectly acceptable for most cases.

1. [11:17 PM]

The ALB -> NAT Gateway flow is just wrong FYI

woods — Today at 11:17 PM

i thought a private subnet is the same as a AZ no?

Bards Aren't Real — Today at 11:17 PM

The ALBs need to talk directly to the EC2 instances and/or the Lambdas, depends on what you're looking for

1. 

Arash — Today at 11:17 PM

aah I see (edited)

1. @woods

i thought a private subnet is the same as a AZ no?

Bards Aren't Real — Today at 11:18 PM

No, a subnet belongs to one and only one AZ, but an AZ can have any number of subnets

1

1. [11:18 PM]

In more advanced VPCs you'll have a bunch of private subnets in a single AZ

1. @Bards Aren't Real

The ALBs need to talk directly to the EC2 instances and/or the Lambdas, depends on what you're looking for



Arash — Today at 11:18 PM

so there should be one nat gateway connected to the alb?

1. [11:18 PM]

and alb connected to ec2 of lambda

1. Icon

   Description automatically generated@Arash

so there should be one nat gateway connected to the alb?

Bards Aren't Real — Today at 11:18 PM

No, the NAT Gateway has no connection to a publicly accessible ALB

1. [11:19 PM]

NAT Gateways only exist for your private resources (eg the EC2 instance in this case) to initiate connections with the internet (edited)

JEF — Today at 11:21 PM

As RDS S3 and lamba are redundant, is it still needed to put them in different AZs? Or does aws do that automatically for us?

Bards Aren't Real — Today at 11:22 PM

S3 is automatically redundant within the region. RDS is not, you need to make sure it's designed for multi-az. Lambda *within a VPC* is not by default either, you need to make sure you give the Lambda function subnets across multiple AZs

1. [11:24 PM]

You can launch Lambda functions outside your VPC (the original way the service worked actually) and it's automatically resilient to AZ outages. But if the Lambda needs access to resources in your VPC (eg your RDS instance) then you gotta launch it in your VPC and ensure the resiliency yourself.

MattheW — Today at 11:25 PM

for a simple arch design, why not just smack RDS serverless v2 on there, no replication BS

JEF — Today at 11:25 PM

So do you think our architecture is ok? Or do you think we should only have 1 S3 bucket instead of 2 (as that is automatically redundant)

Bards Aren't Real — Today at 11:27 PM

Oh right, you do have S3 buckets in your VPC. Yeah that's wrong too; not how S3 works. CodeBuild and Cognito being in your VPC also isn't right

Serhad Aras — Today at 11:28 PM

So codebuild and cognito need to be outside of the VPC but also outside the region rectangle?

Bards Aren't Real — Today at 11:29 PM

No, they are within a region just not within a VPC. Almost every service in AWS is regional, IAM being the big exception

MattheW — Today at 11:31 PM

also is the intended behavior for codebuild to deploy to EC2 directly? instead of the codeDeploy service

1. @MattheW

also is the intended behavior for codebuild to deploy to EC2 directly? instead of the codeDeploy service

Serhad Aras — Today at 11:33 PM

We don't need to deploy any of the code that is been sent to CodeBuild. We only need to get an response of the execution of the code.

1. [11:38 PM]

So we also need auto scaling do we need to use it for the whole AZ or only like the EC2 and the RDS