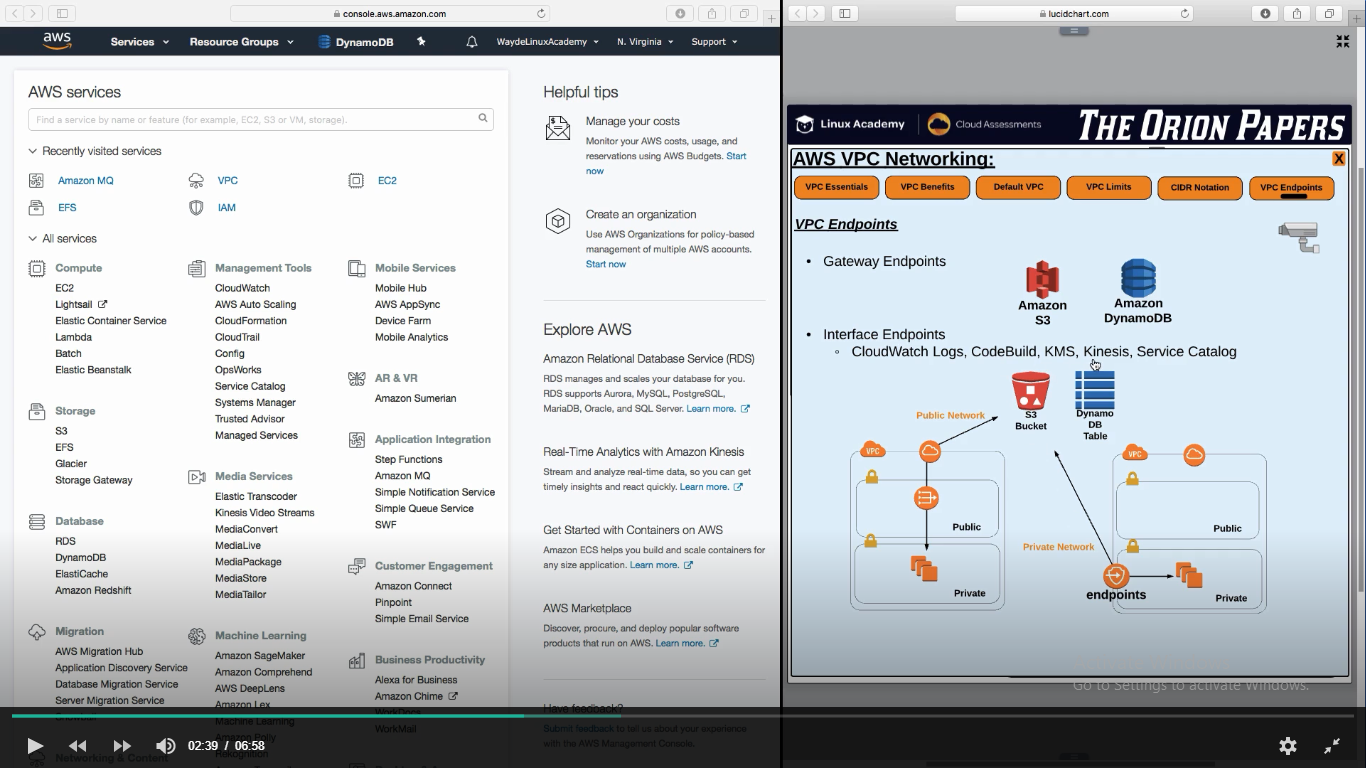
**VPC Endpoints**

**Why VPC Endpoints:**

If we want private subnet instances (EC2) to access AWS public service (ex. S3) over public network. Sensitive data’s are not allowed to access via public network. Hence we have VPC Endpoints

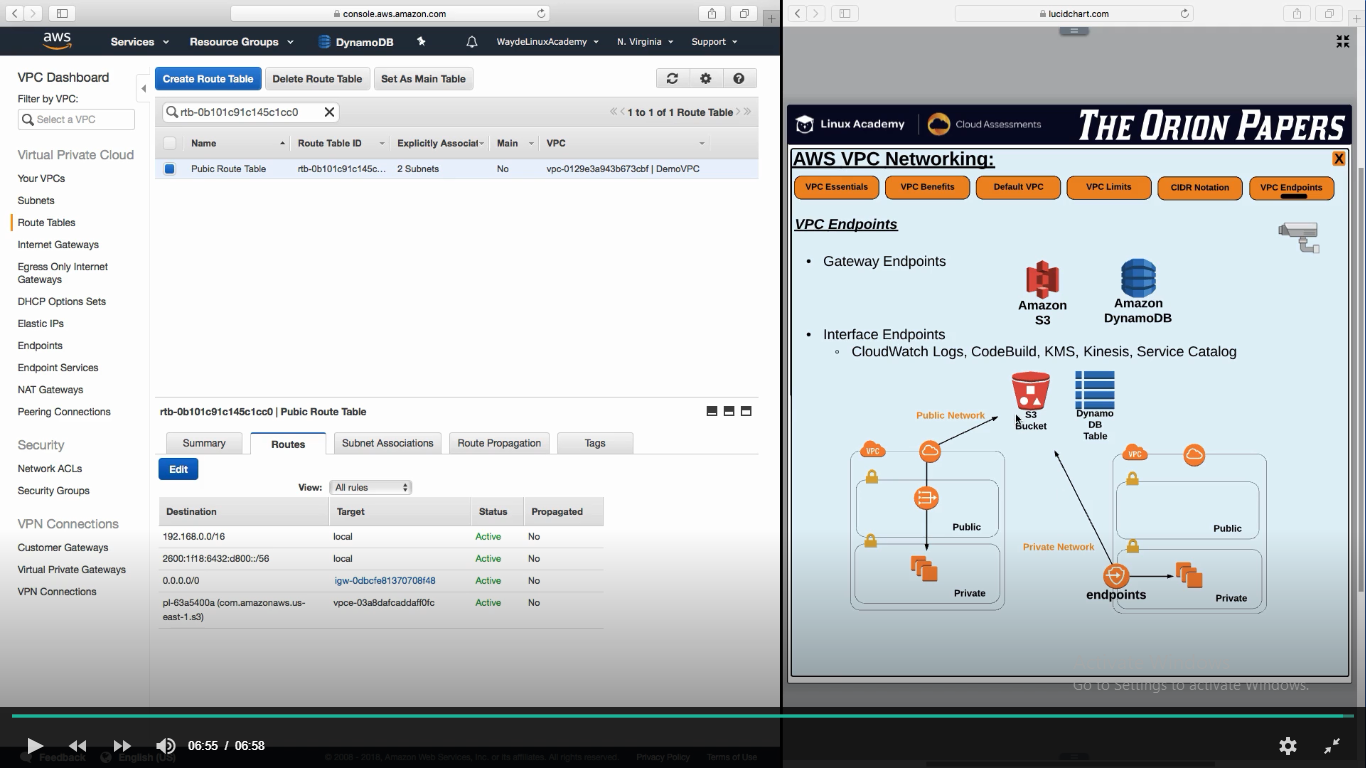
There are two types of Endpoints

1. **Gateway Endpoints**
   1. Drop the endpoint in the subnet
2. **Interface Endpoints**
   1. Uses elastic interface to communicate with the services



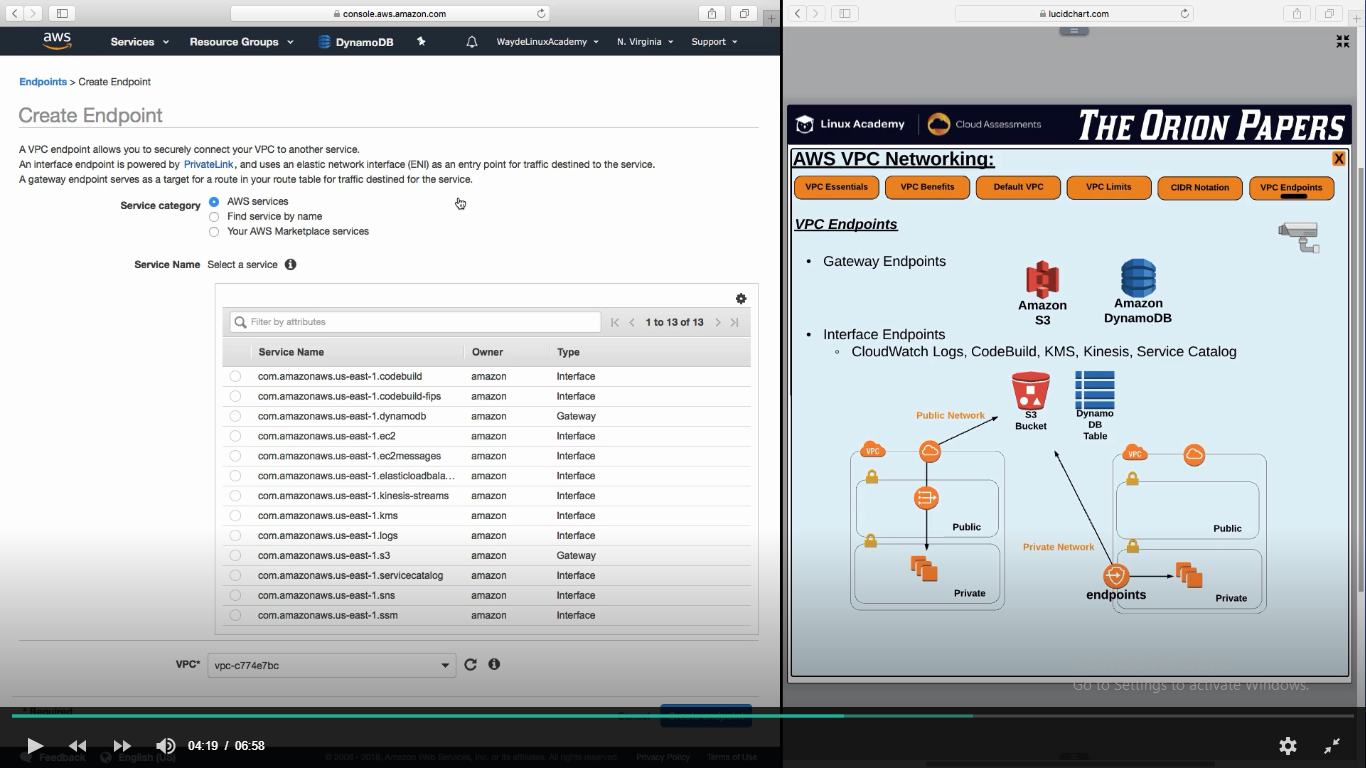
Creating endpoint for S3 and associating it to VPC and subnet

S3 bucket policy we left as it is as it can be managed by S3 bucket policy or via AIM user policy

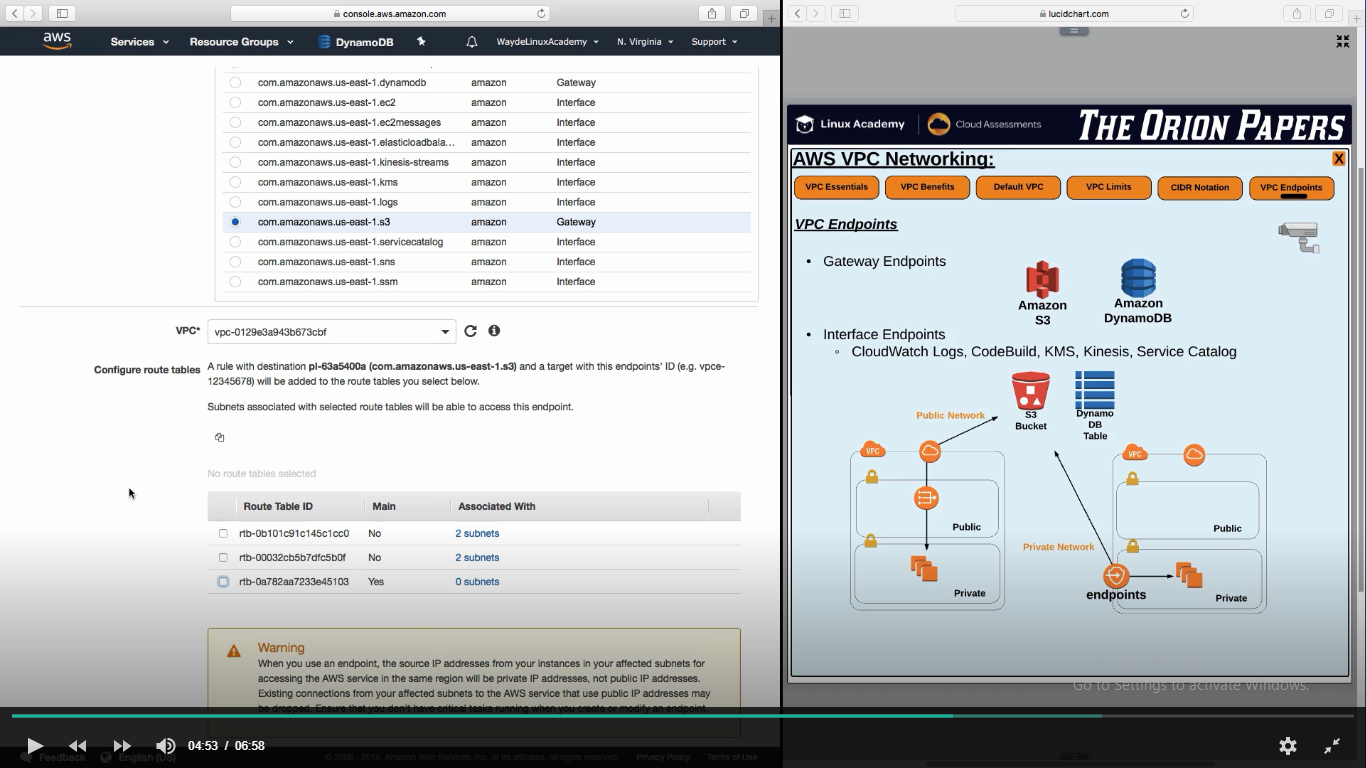


**Creating an Endpoint**

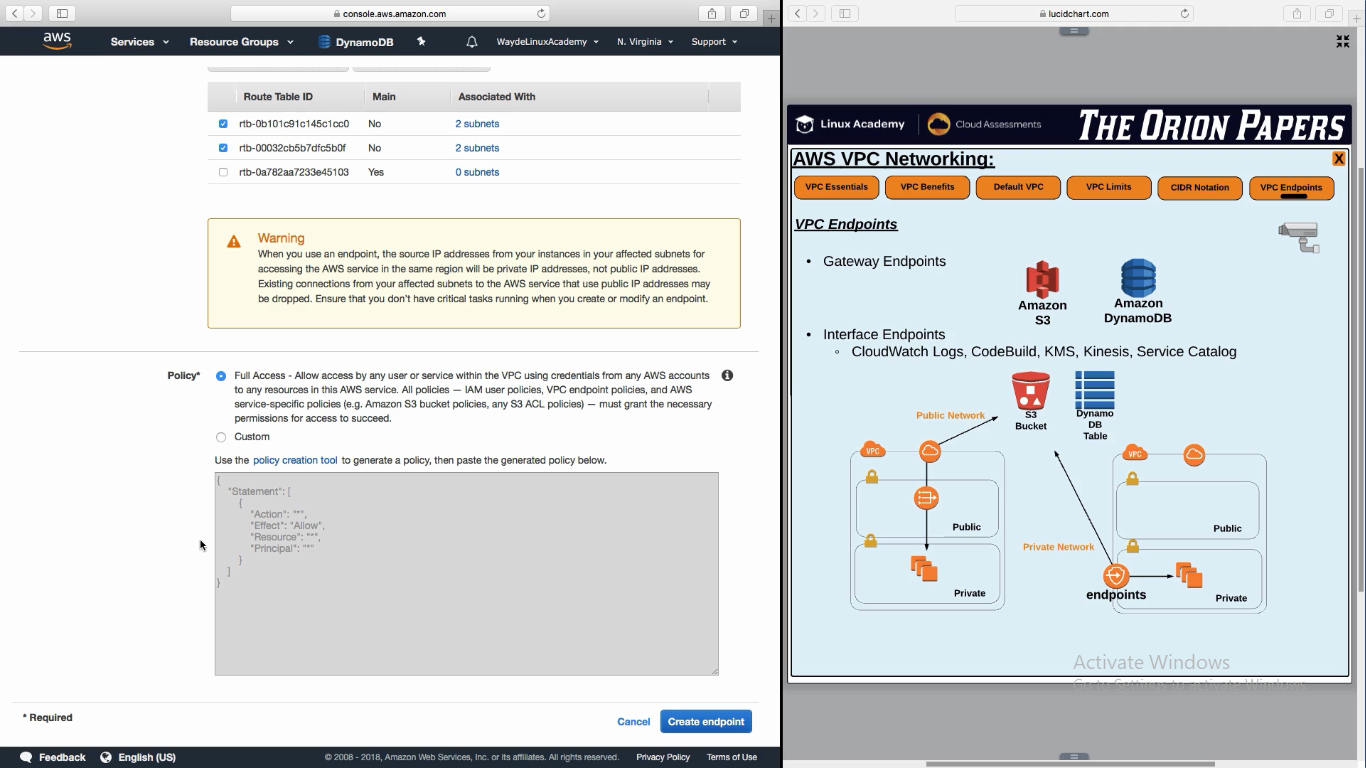
1. Console -> VPC -> Endpoints -> Create Endpoints
   1. We are going to create a endpoint for S3 and put it in VPC and see how route tables are adjusted to route the request to VPC endpoint and not through the internet gateway
2. Select service category and the name of the service we want (Eg. S3)



1. Attach VPC
   1. Once attached, AWS will automatically create the destination alias and is automatically going to be added to the route table. So that reques will go via endpoint to S3



1. Attach a IAM policy
   1. Which bucket can be accesses
   2. Mostly we will give full access/default policy



Click create endpoint