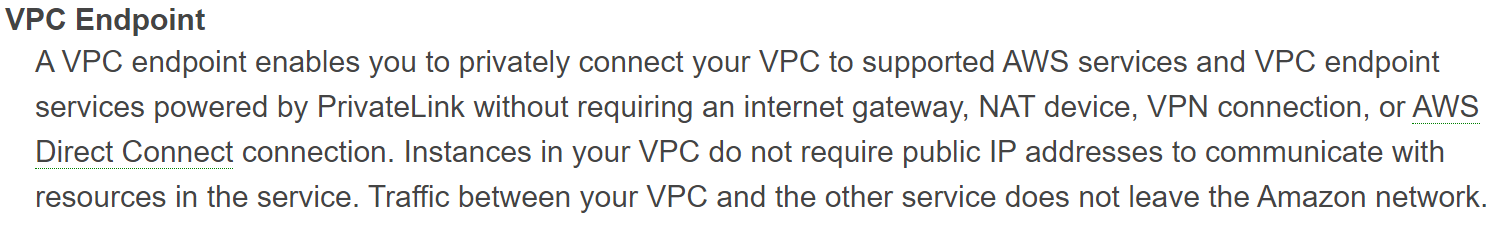
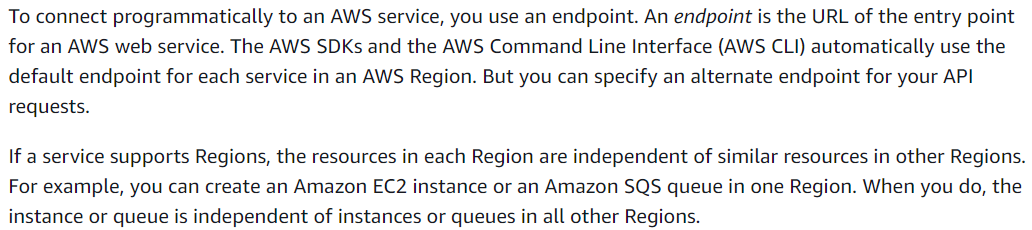
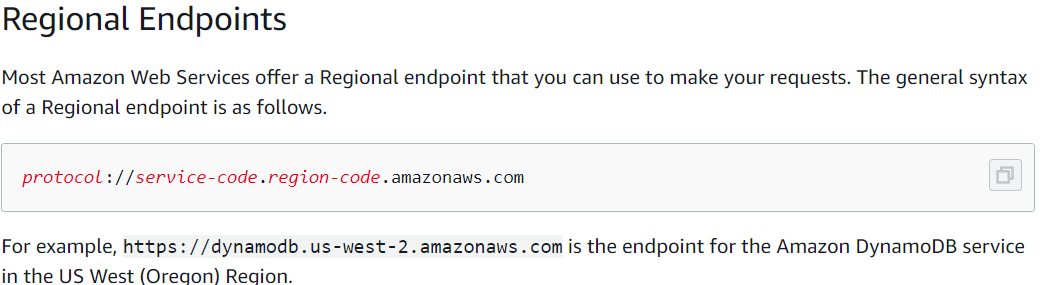
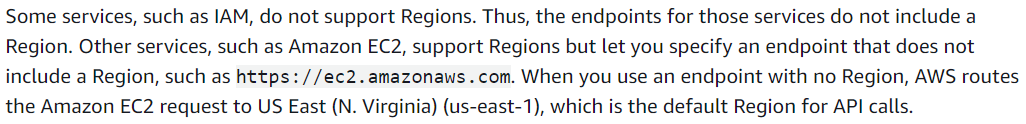
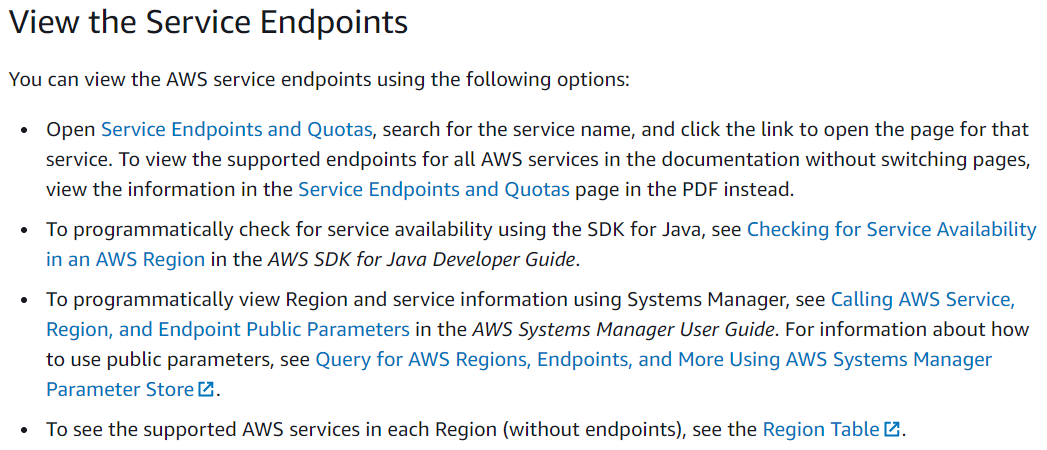
**Introduction:**

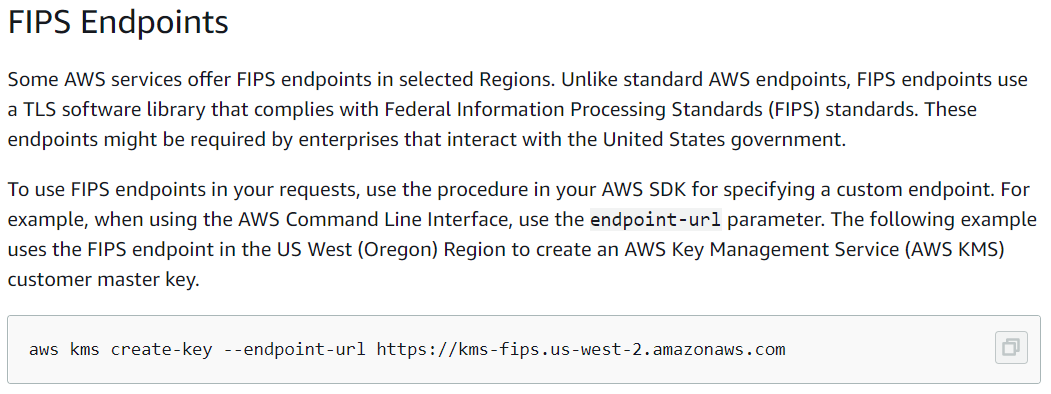




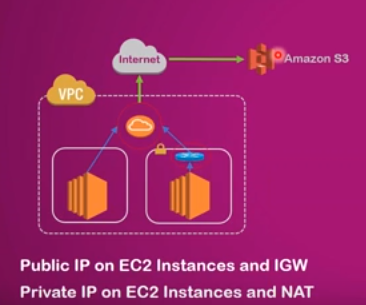








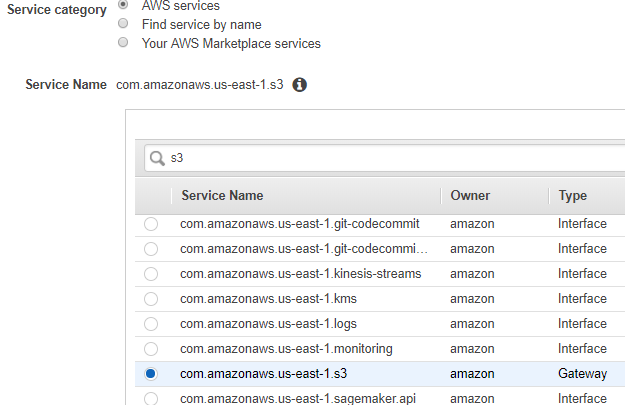
**Practical:**



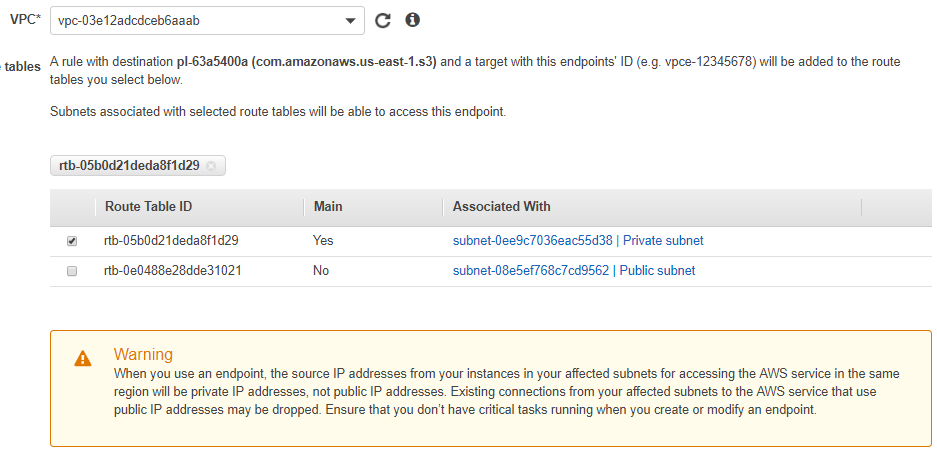
* If private IP wants internet connection, then we need to have NAT gateway



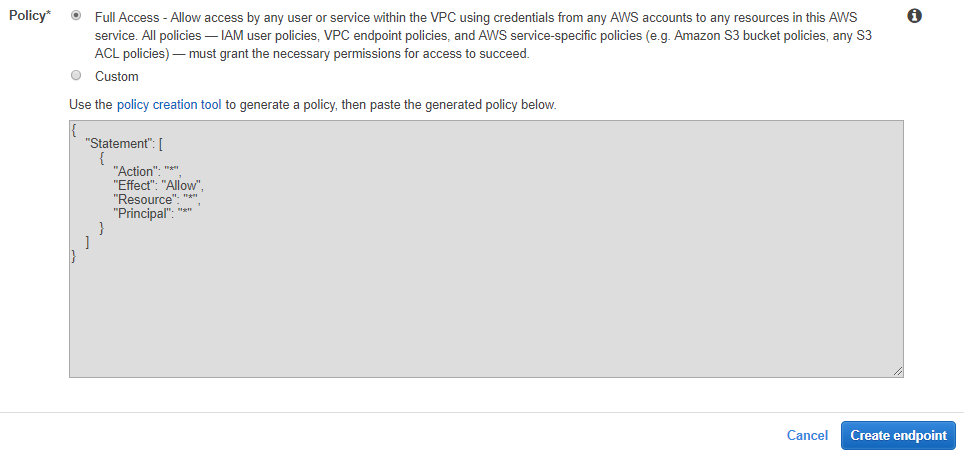
* Endpoint can have private connection with S3
* Create a public instance with the role to access s3 bucket
* The private instances cannot access the S3
* Once we create the endpoint, the communication between ec2 instance and s3 will happen using amazon’s private network
* We can create these endpoints to s3 for an ec2 instance of VPC which is in same region. We can not do it for another regions
* Earlier, the endpoint is for s3 only. Recently it came for other services also



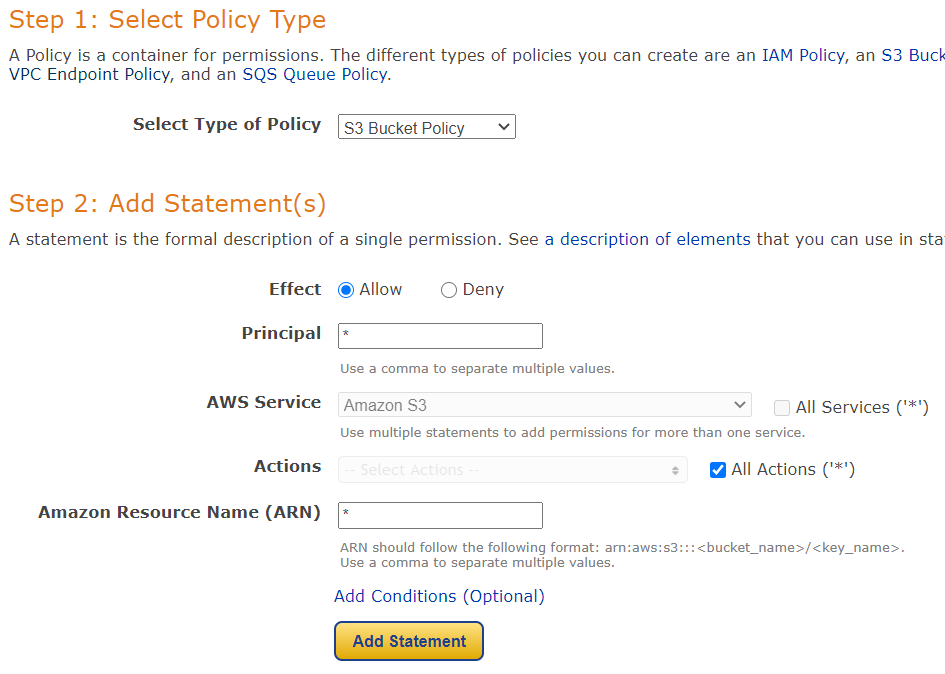
* Now create an endpoint with region and the service as above



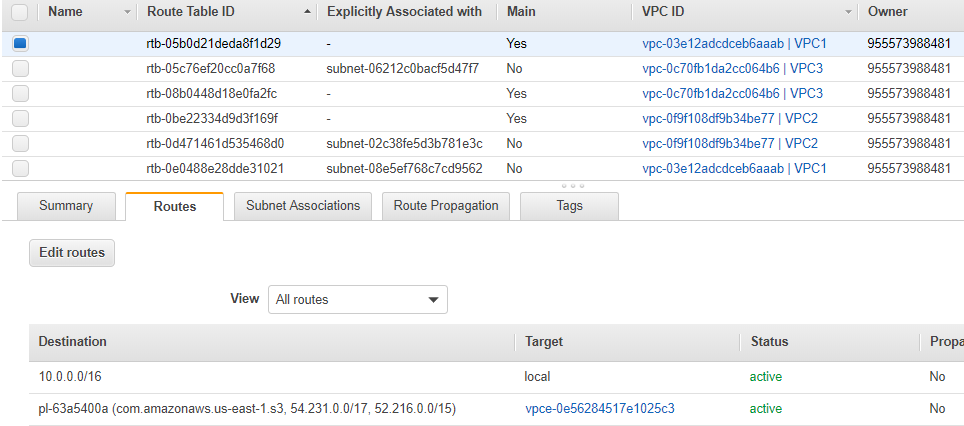
* Select the VPC, and go for private subnet’s route table as above
* Read the warning message before proceeding further



* Enable the policy also
* If we want to create custom policy, we can create it with policy generator tool as below



* As above, we need to select the policy as “s3 bucket policy”. Principal we may can add “\*” and the services we need to add to which the connection is required. If to all the services, we can add ‘\*’
* ARN number, we need to add if the access is required to be enabled to some particular bucket or we can give \* for all the buckets



* Now we can see there is an entry at route tables under private subnet
* If it’s not getting updated, under endpoint click on manage route tables and save it once
* As per the entry above under route tables means if the traffic comes for that, it will route to that endpoint
* We can check now from private instance using s3 commands

**The s3 bucket and VPC should be in same region. There is no charge for this because it uses amazon’s private network**