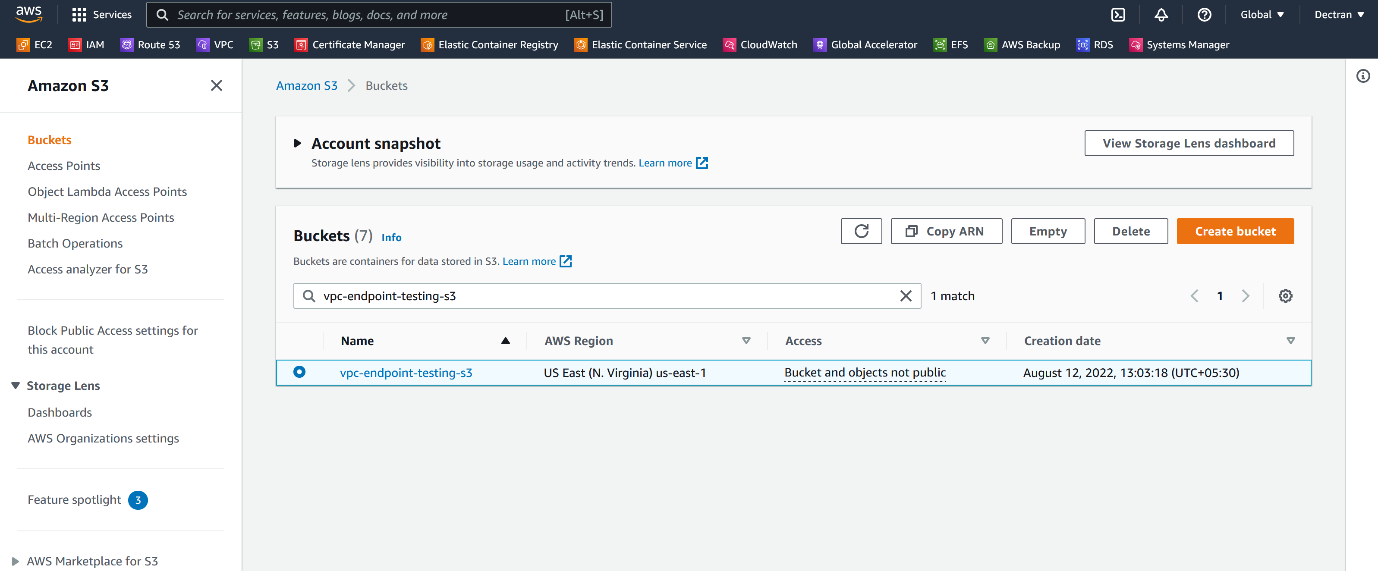
**07.AWS-B30-EndPoints**

--- in this session, we will talk about vpc endpoints.

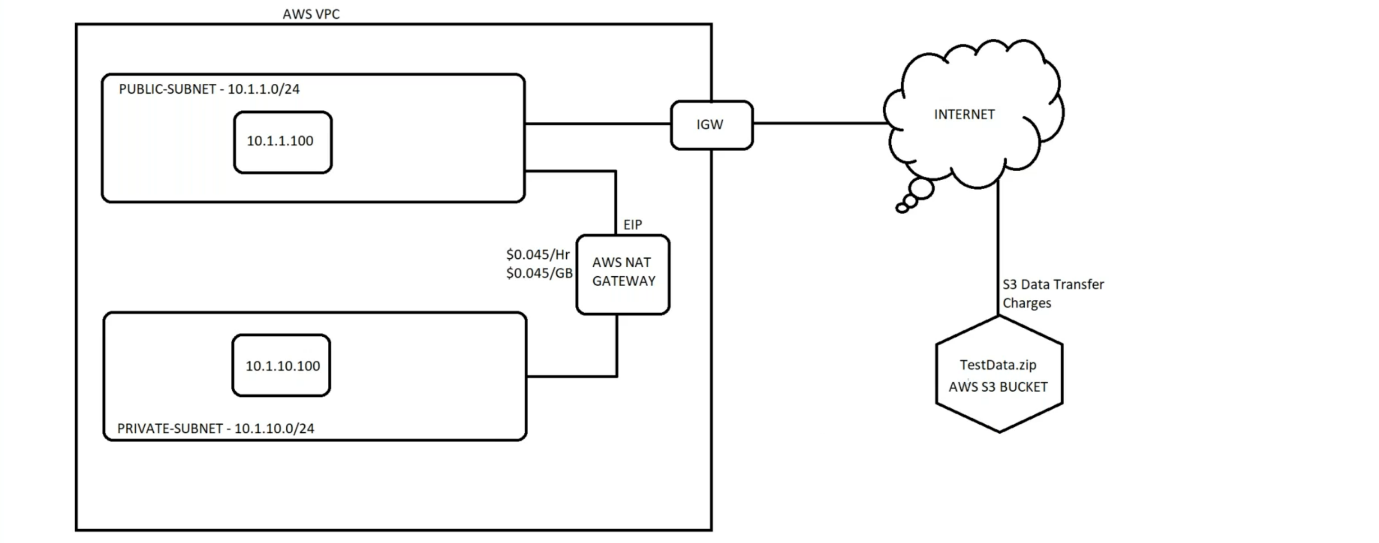
**Create s3 bucket in s3**

--- **prerequisites** – create bucket in s3



--- **note** – I have created a bucket called vpc-endpoint-testing-s3. This bucket is used to test **endpoints**.

**Vpc end point architecture**



--- **scenario** – your application is running in a private instance. Application is accessing the internet via **AWS NAT GATEWAY**. The nat gateway charge you **$0.045/Hr** and data charge is also same. If your application is accessing the date which is present inside of s3 over the internet then you need to pay money for data transfer. If you establish connection between application instance and s3 internally using vpc endpoints then you do not have to pay date charges because the data transfer will happen internally.

--- **NOTE** – **AWS NAT GATEWAY** is used for downloading packages etc… for internal usage like downloading files s3 we will use endpoints.

--- **what is your VPC end point…?**

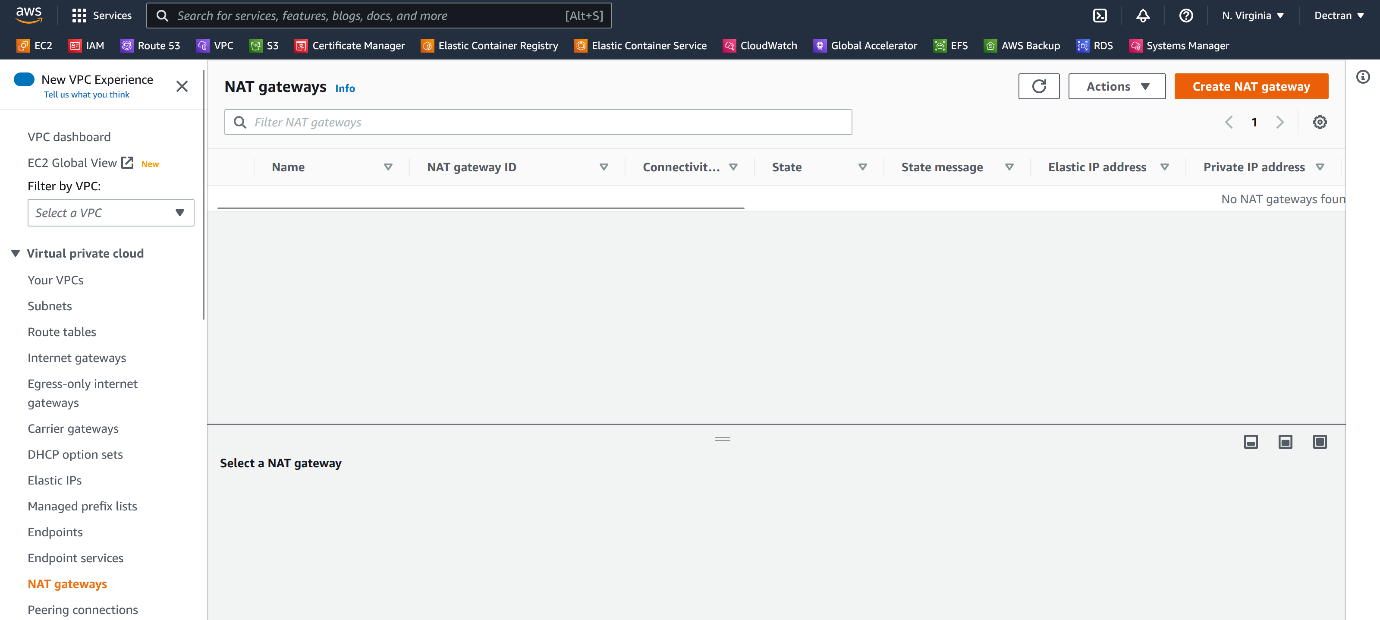
from your vpc, most probably form ec2 instances to connect other aws services. This process is called vpc endpoints.

--- **types of aws vpc endpoint…?**

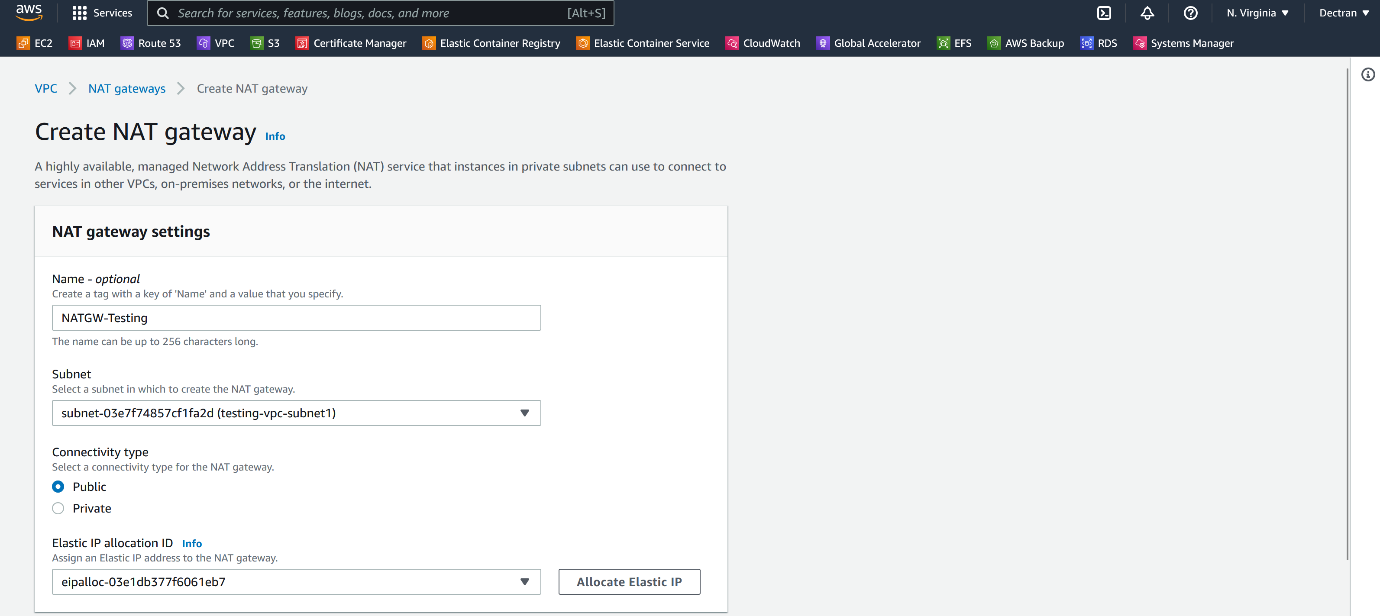
1. Gateway endpoint – it will add route to words s3 in the routing table.
2. Interface endpoint – it will create network interface.

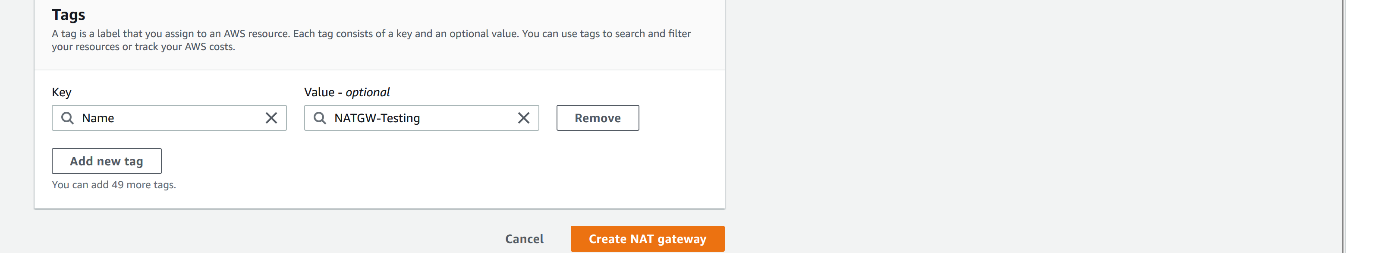
**NAT GATEWAY Creating**

--- go to VPC and click on NAT GATEWAY.



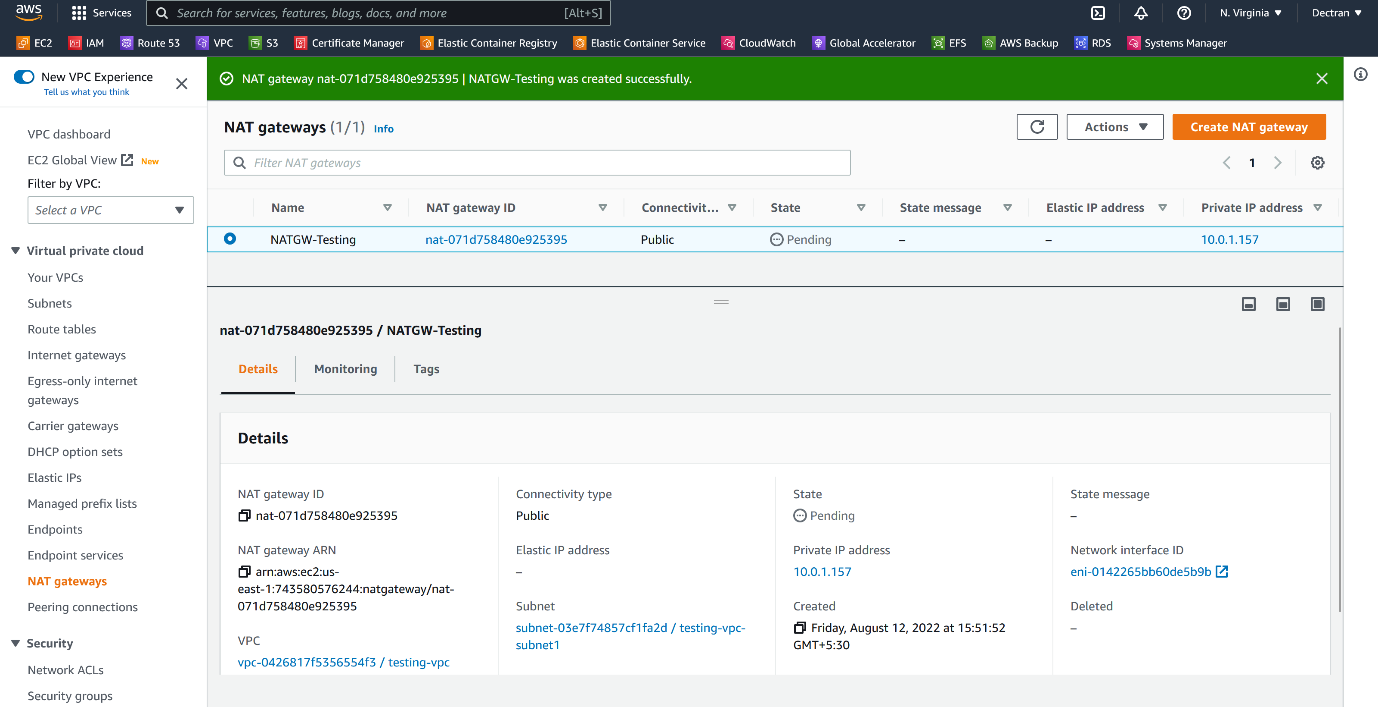
--- Click on create NAT GATEWAY.





--- if you have elastic IP then please give that ip address here.

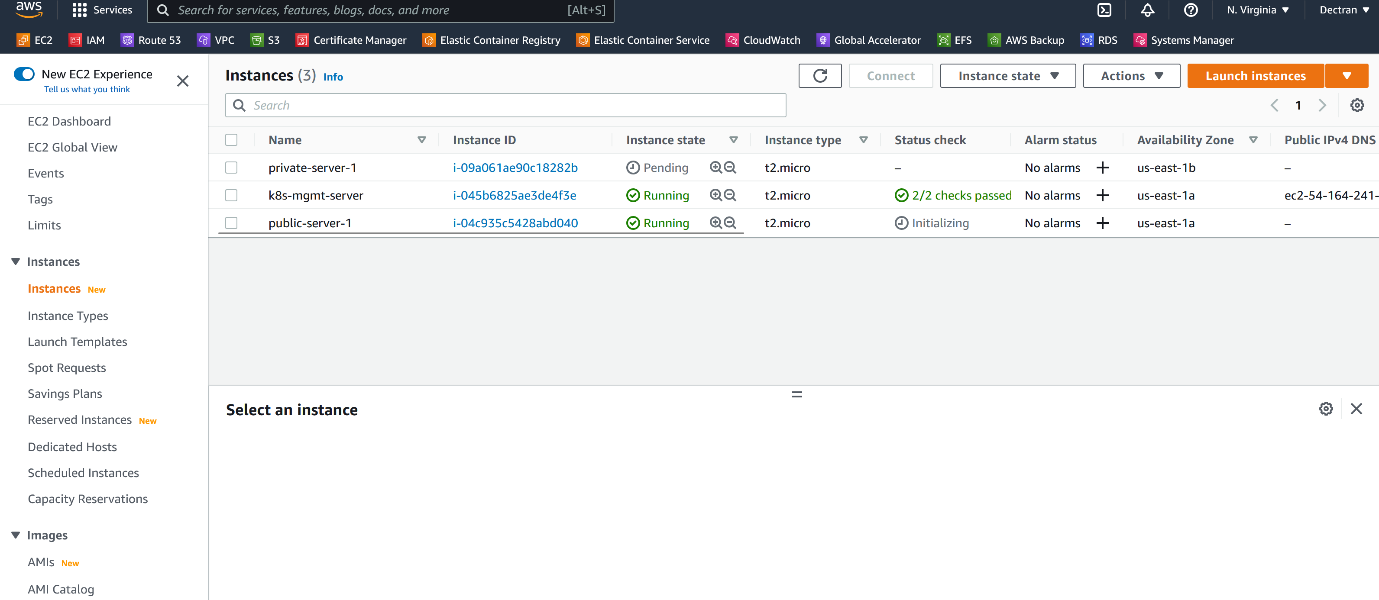
--- click on create NAT gateway.



--- our NAT gateway got created.

**Create 2 servers**

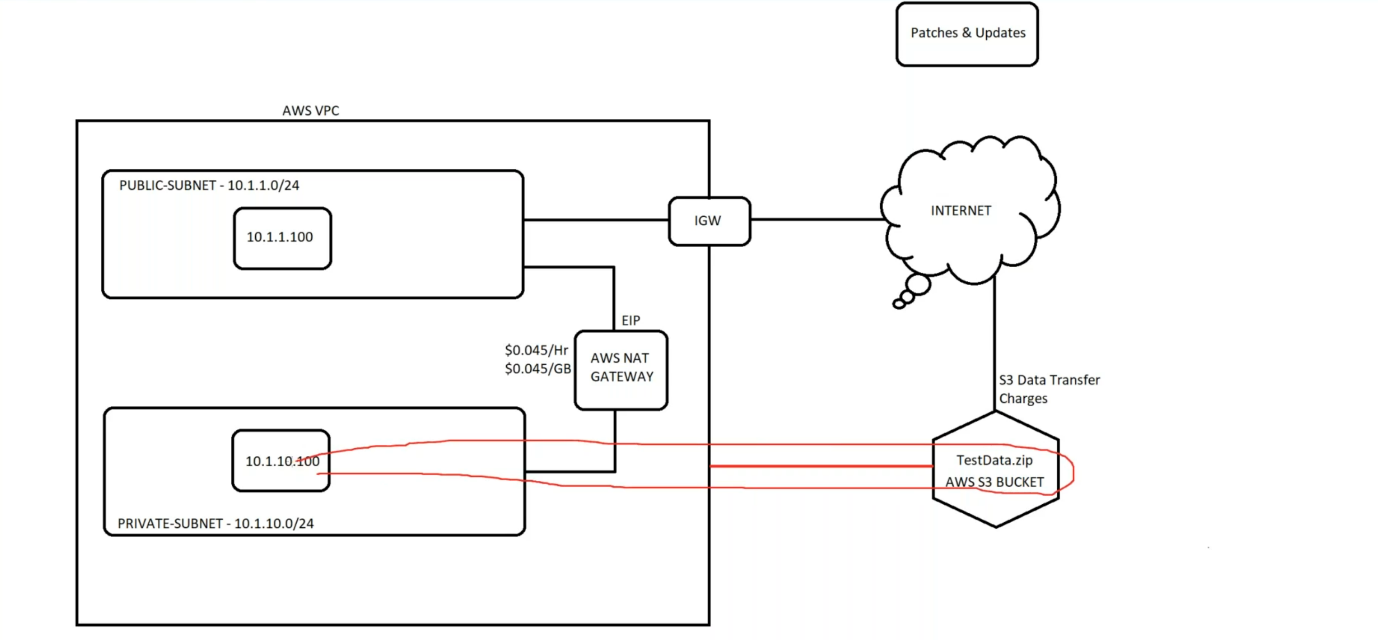
--- **note** – I am going to create single private and single public servers.



--- **note** – created public and private servers.

--- **note** - **public-server-2** communication is happens through internet gateway and **private-server-1** communication is happens through nat gateway.

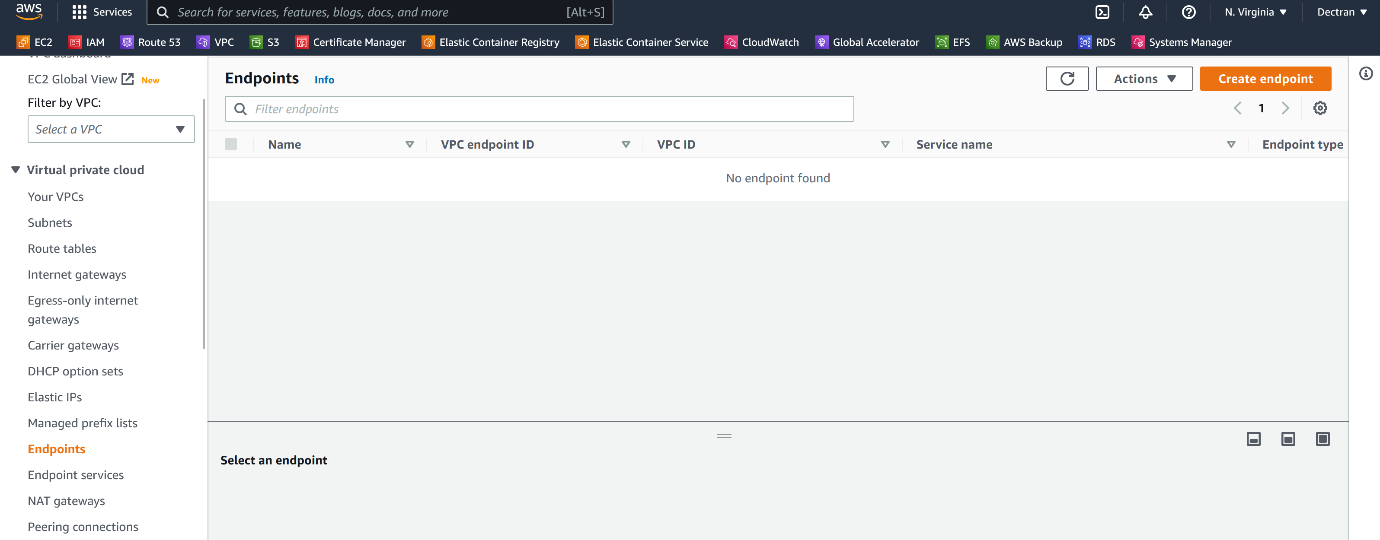
**Gateway endpoints creating**



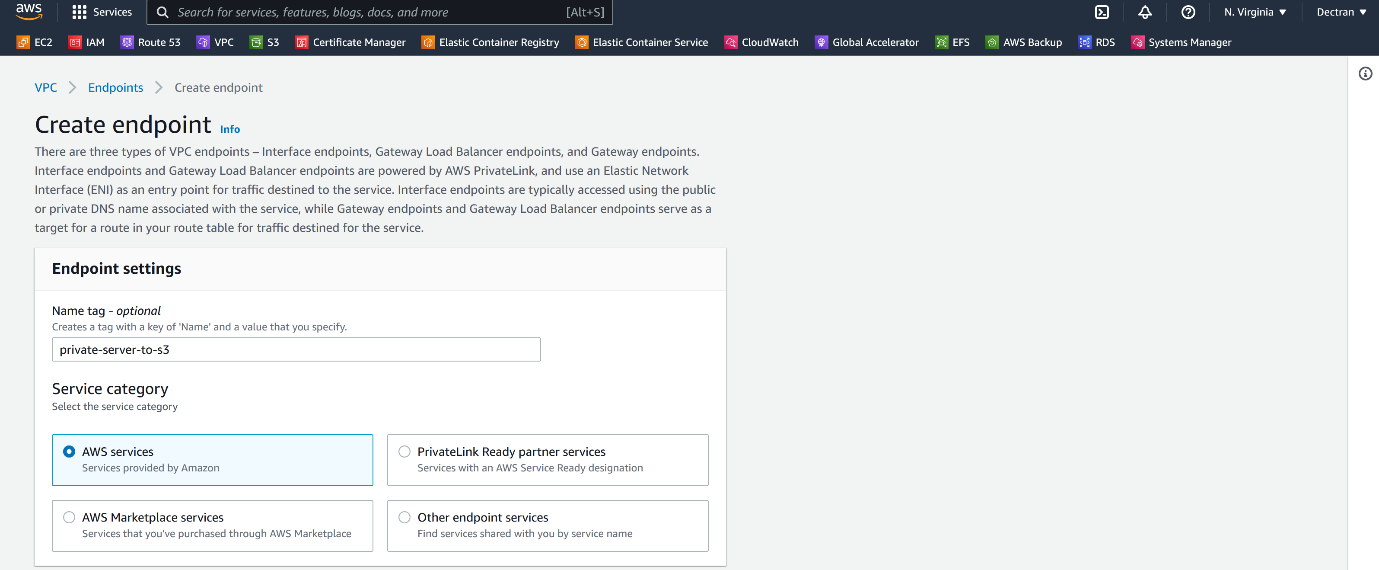
--- **note** – we need to establish connection between s3 and private instance internally.

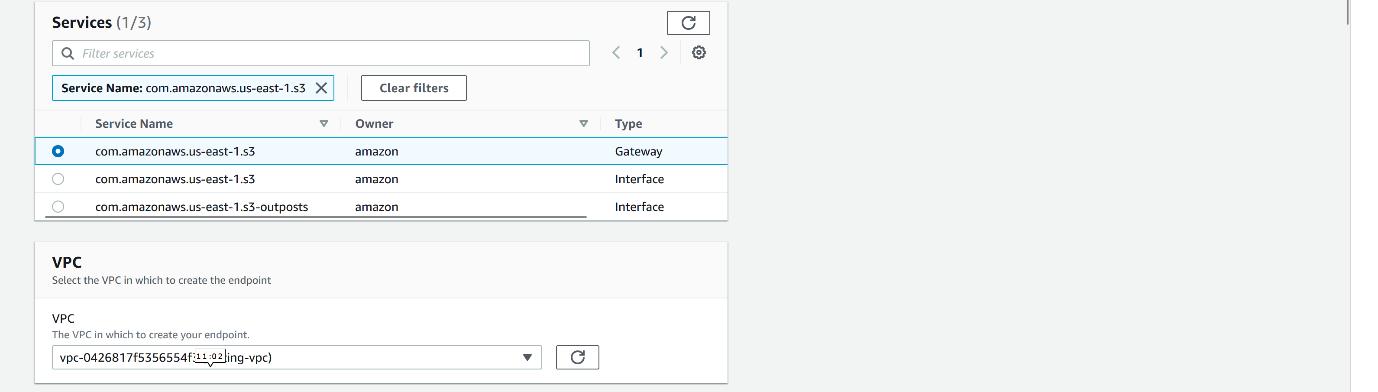
--- **note** – endpoint is region base.

--- go to aws vpc and click on endpoints.

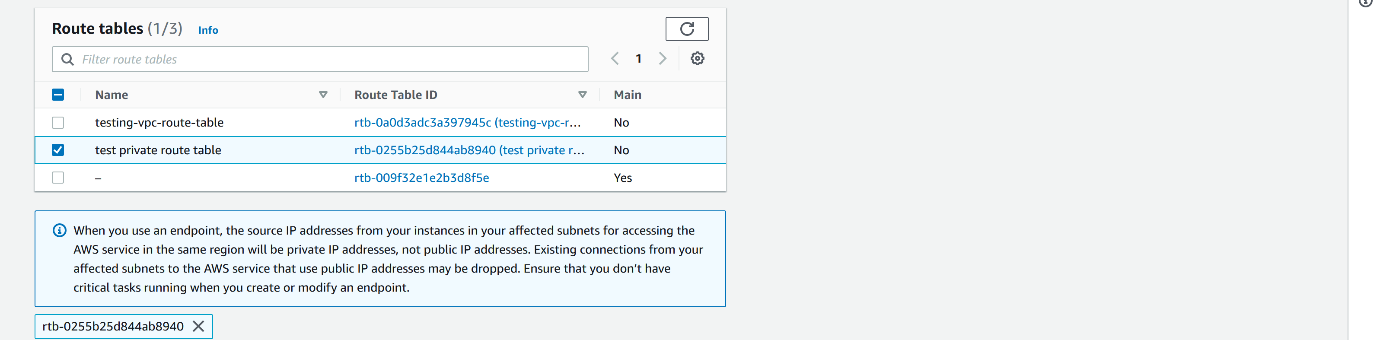


--- click on create endpoint.

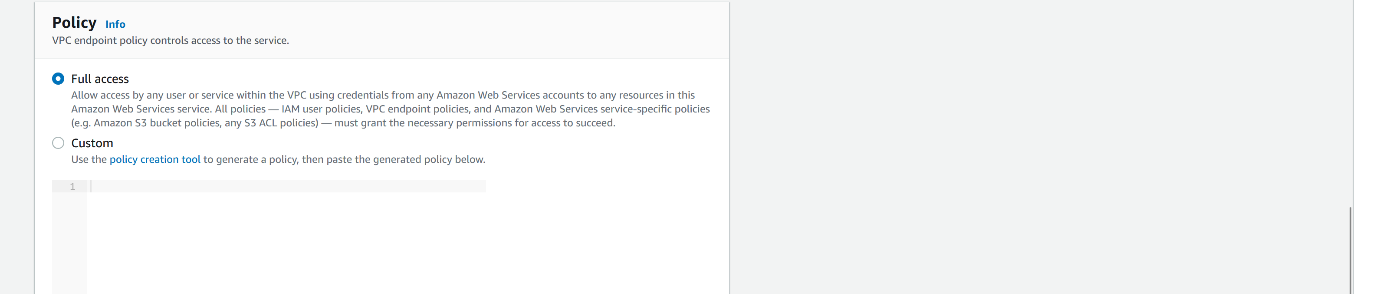


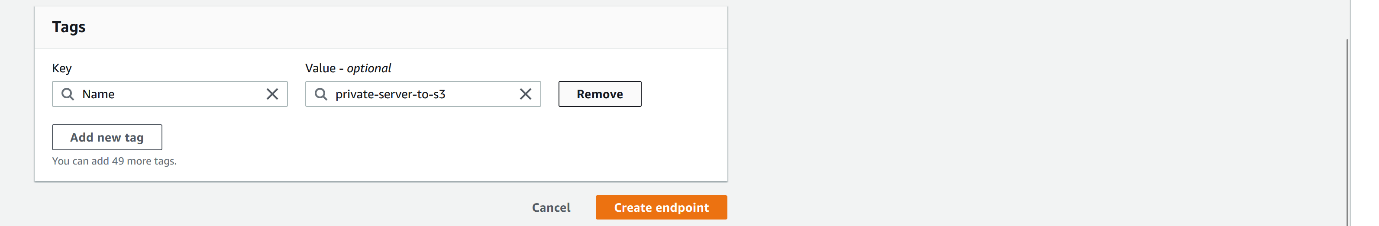


--- please select the vpc that your private instance is in.

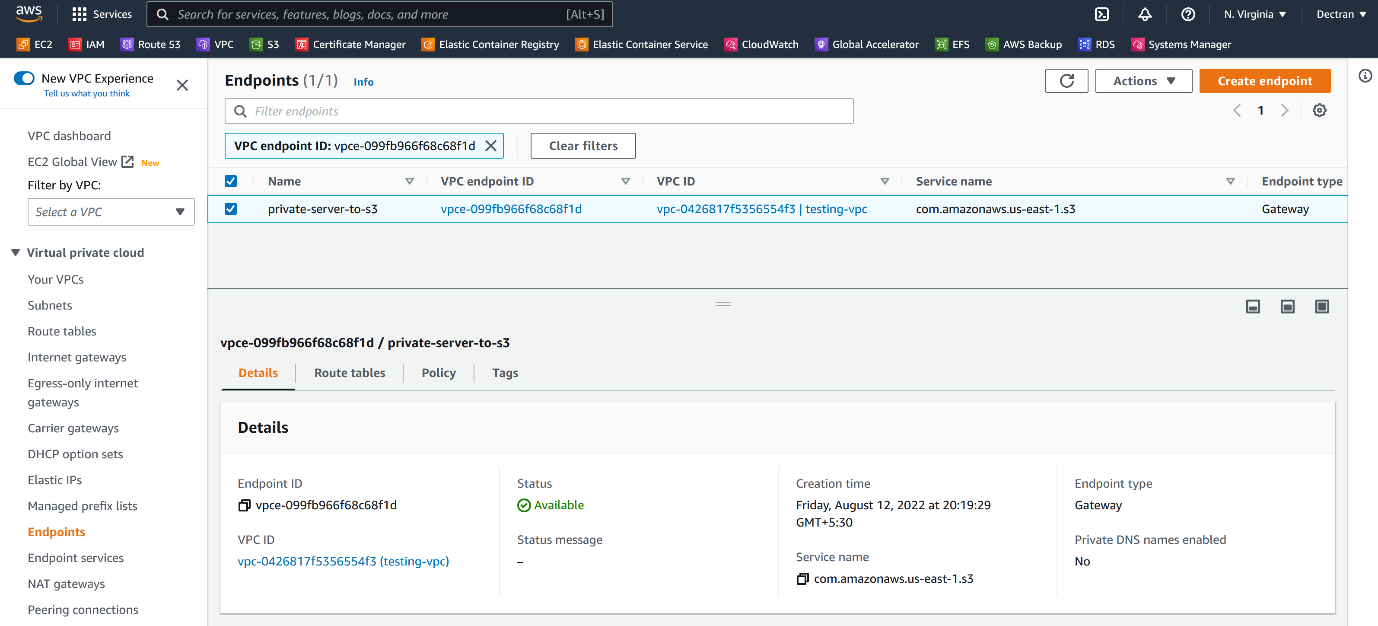


--- please select the route table that your private instance is part of. My private instance is present in private route table that is why I selected this route table.





--- click on create endpoint.

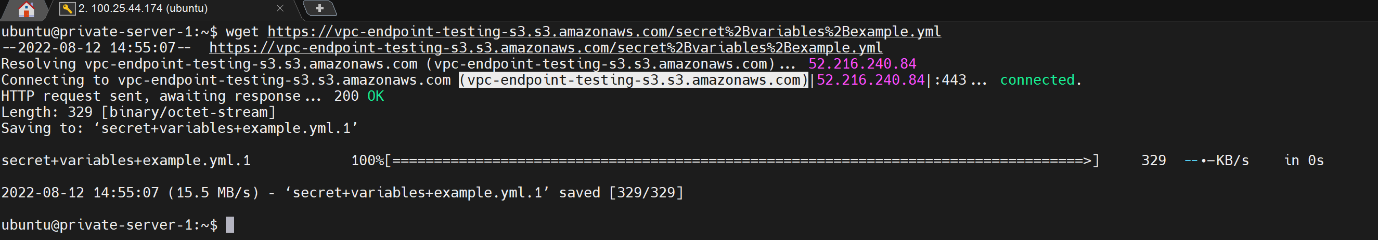


--- our endpoint is created.

--- **important** – please remove the route table which is associated the private instance.

**# Login to private-server-1 and try to download the file**

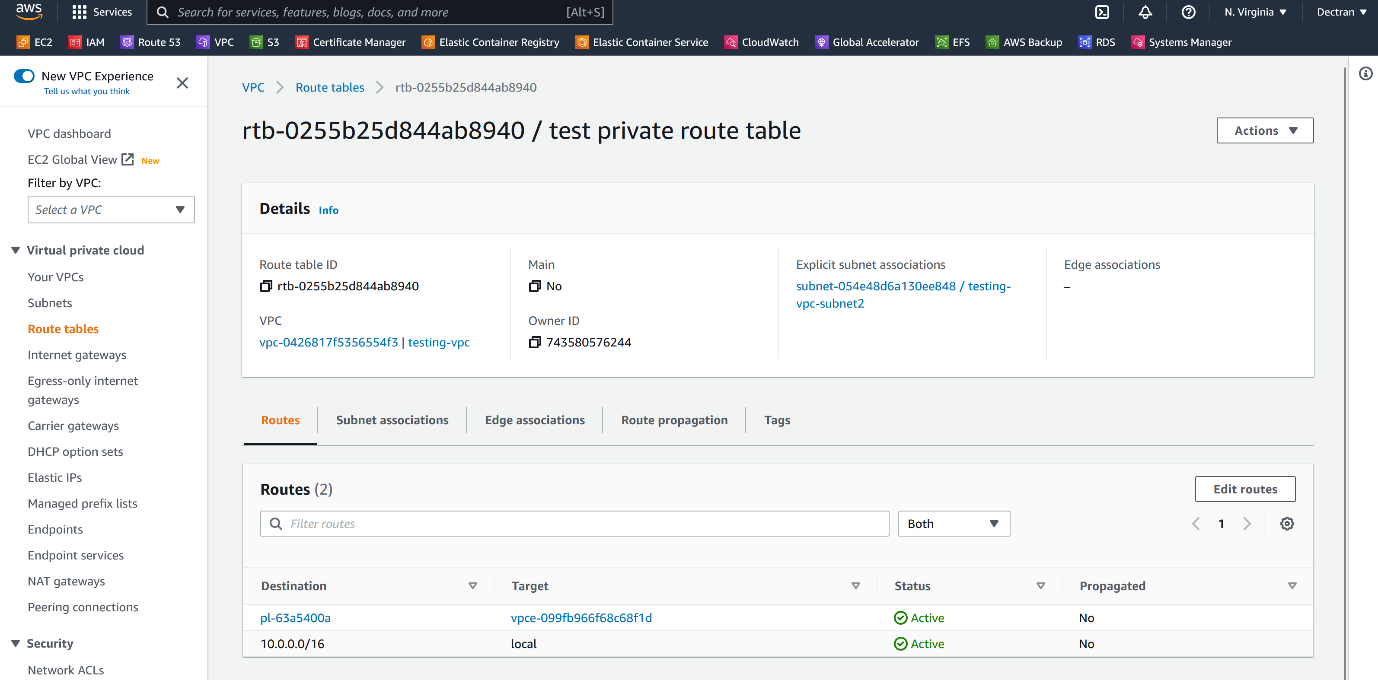
--- wget https://vpc-endpoint-testing-s3.s3.amazonaws.com/secret%2Bvariables%2Bexample.yml



--- **NOTE** – we are successfully established connection between s3 and private server.

**# Check private route table of private instance**

--- go to aws private route table section.



--- **note** – end point is added in private route table.

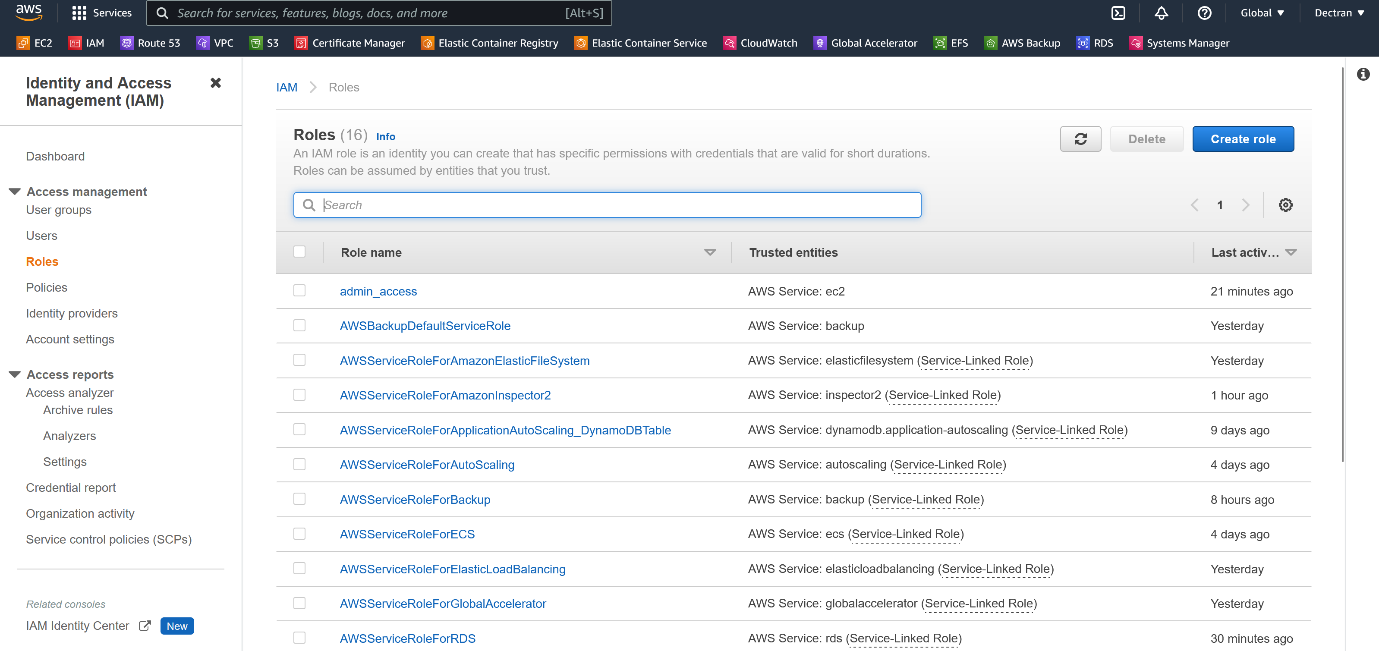
**Login to a server without keys**

--- **scenario** – we have a server that we lost all the keys and password, authentication on that server is not enabled then how do we login.

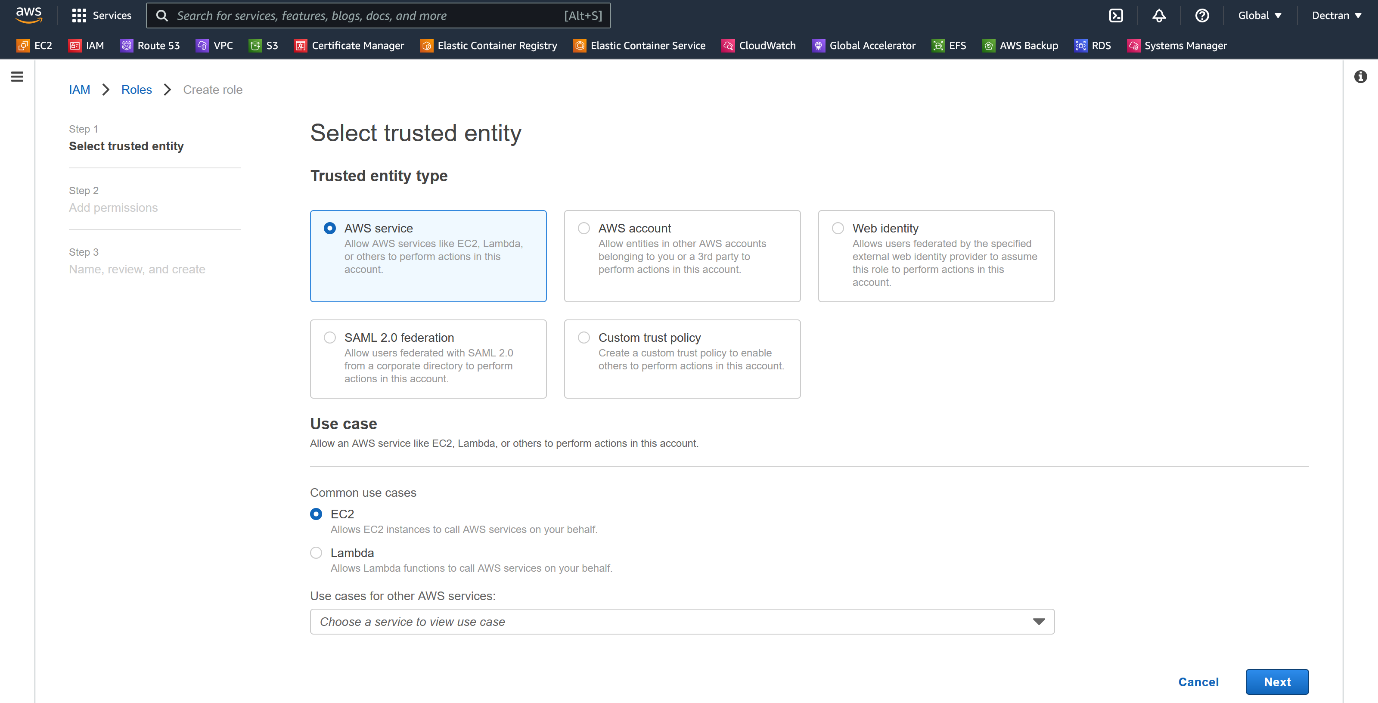
--- **important** – using session manager we can connect to public server but not private server.

**Create a IAM Role**

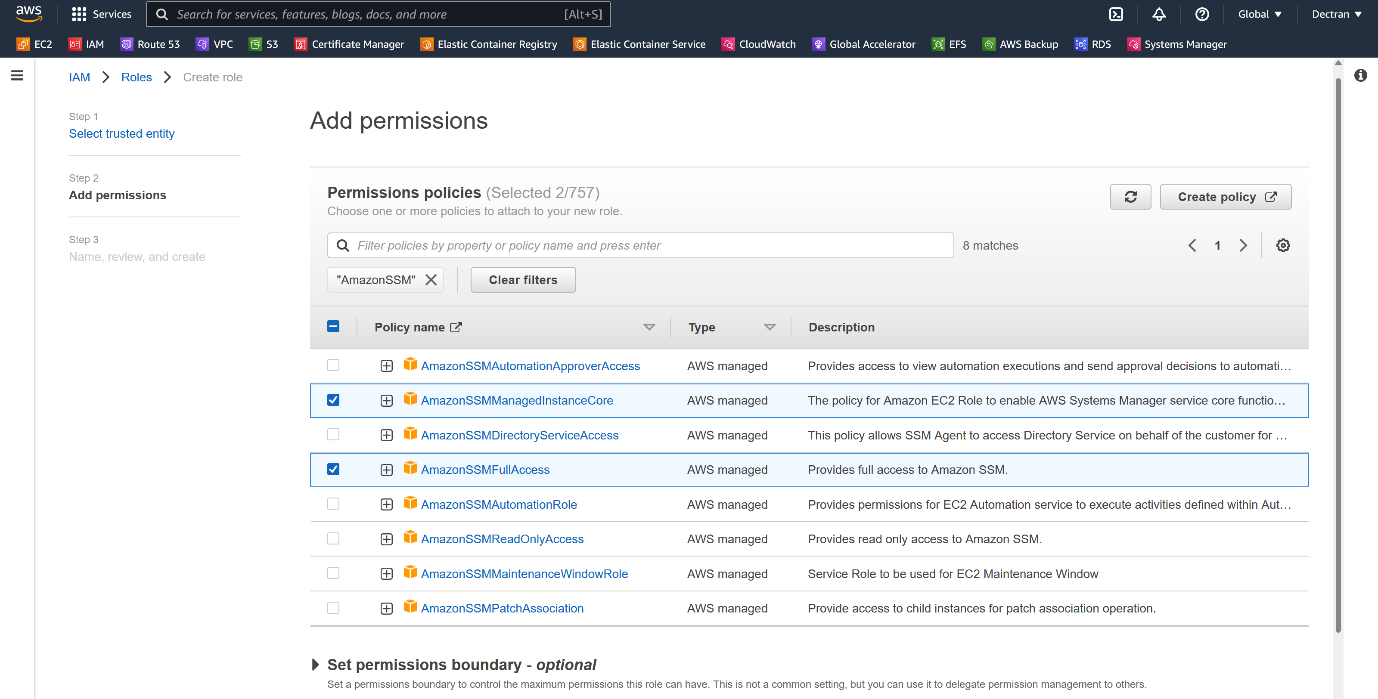
--- go to IAM Role.



--- click on create a role.



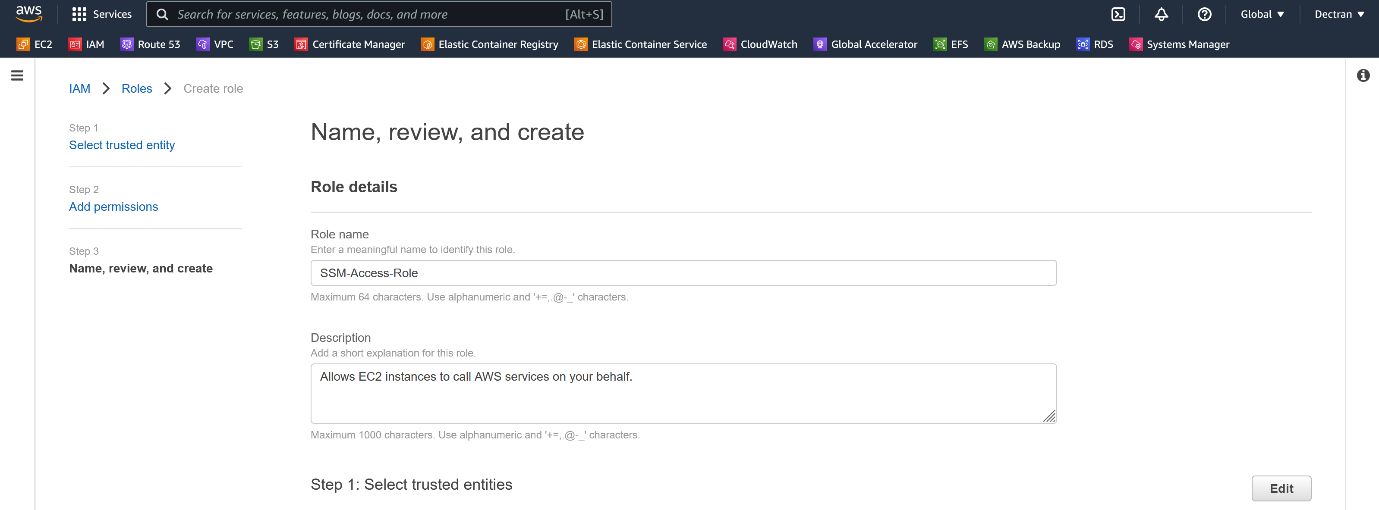
--- click on next

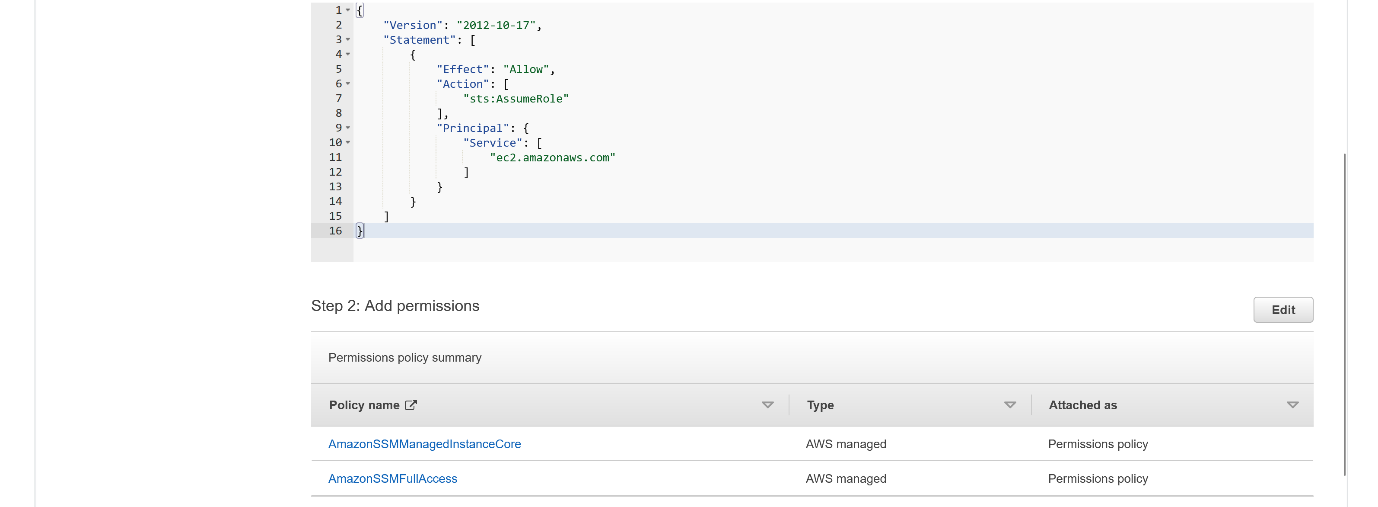


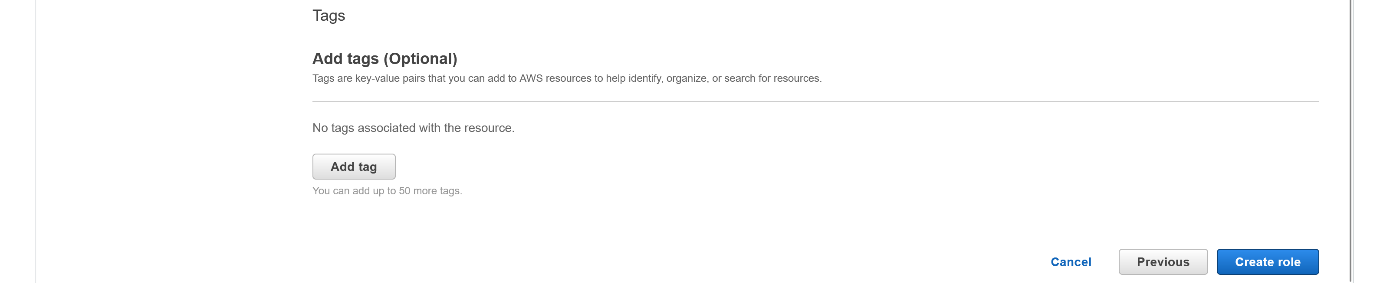
--- **NOTE** – Please attach these 2 policies

1. AmazonSSMFullAccess,
2. AmazonSSMManagedInstanceCore,

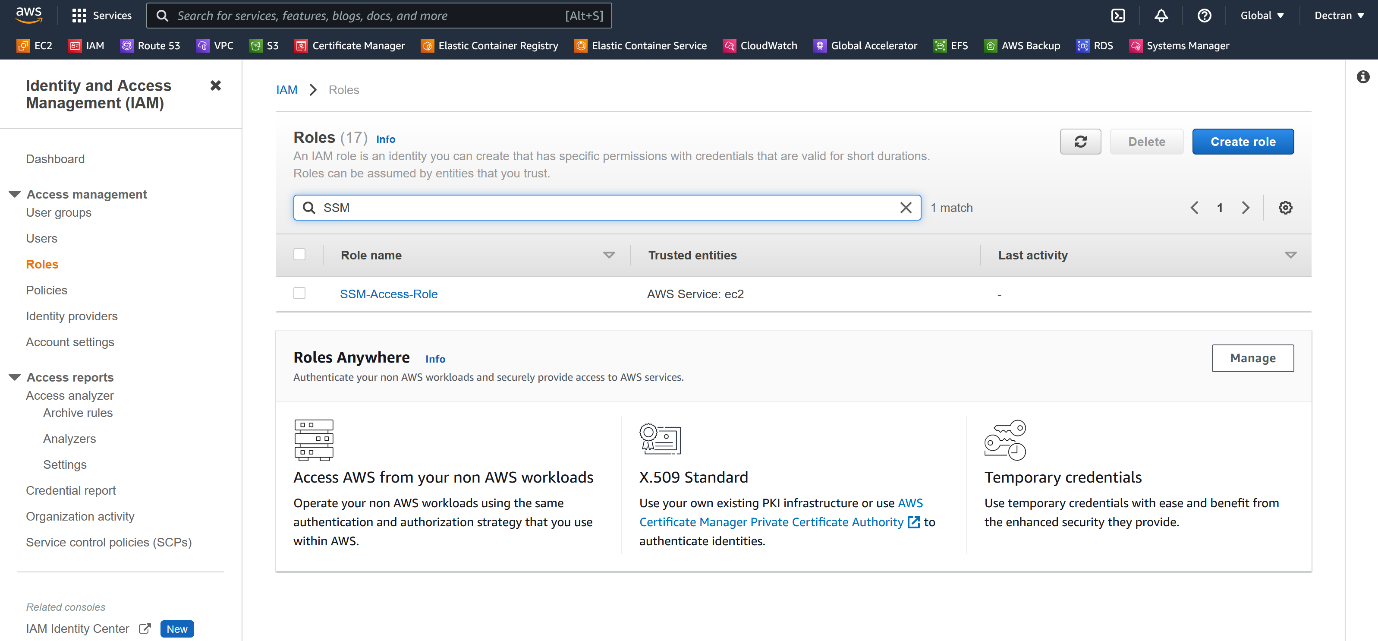
--- click on next and create role.





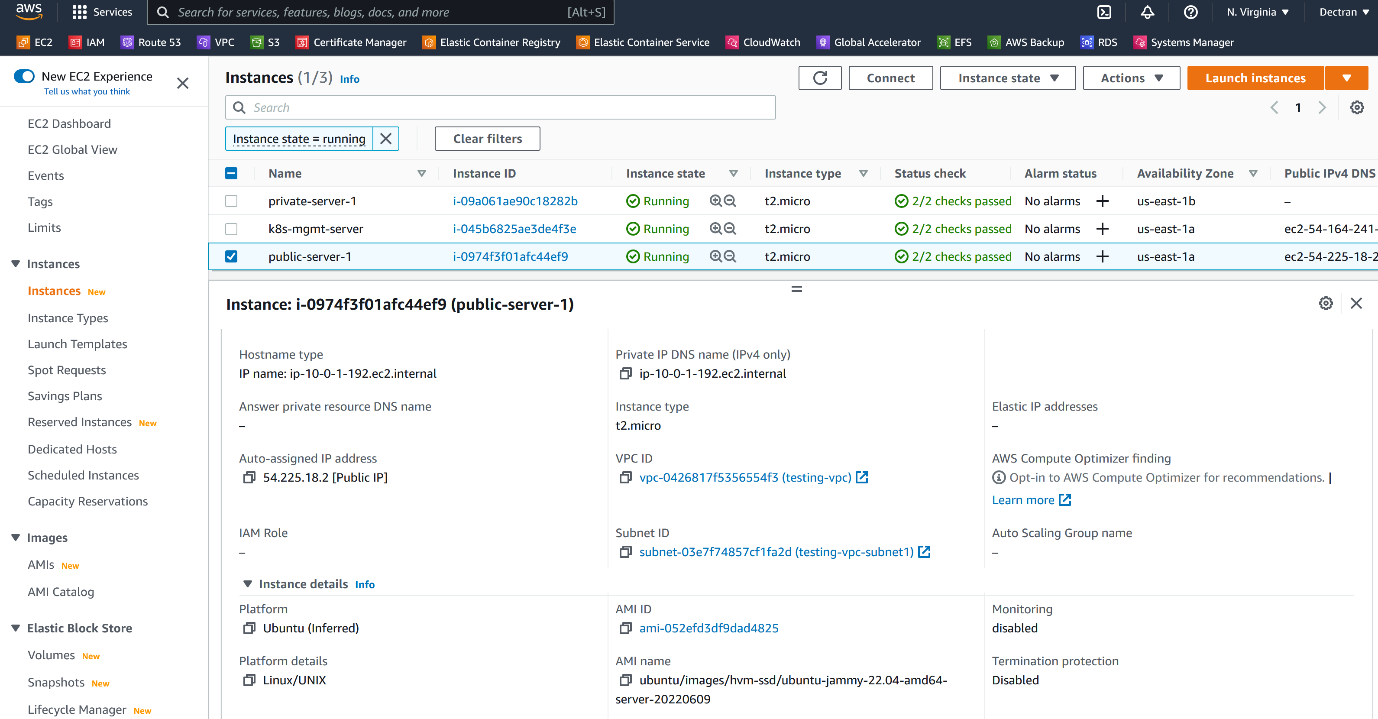


--- click on create role.

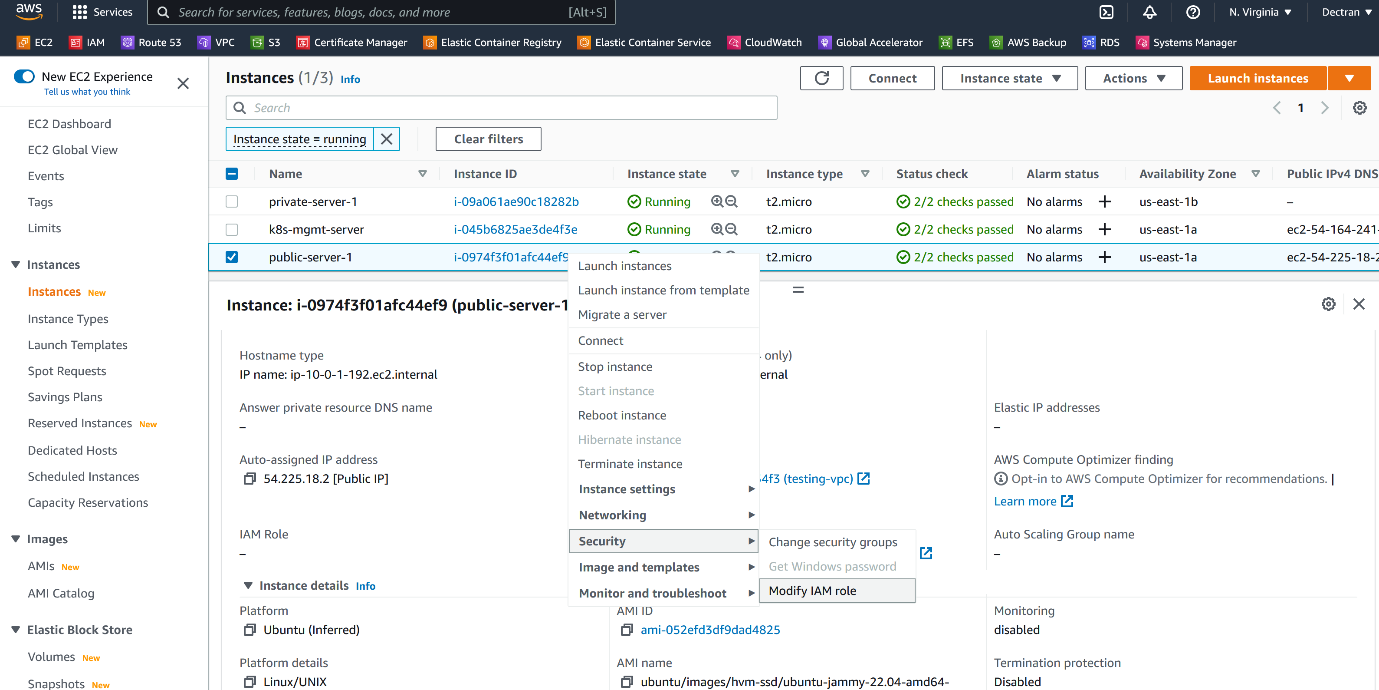


--- **note** – our SSM-Access-Role got created.

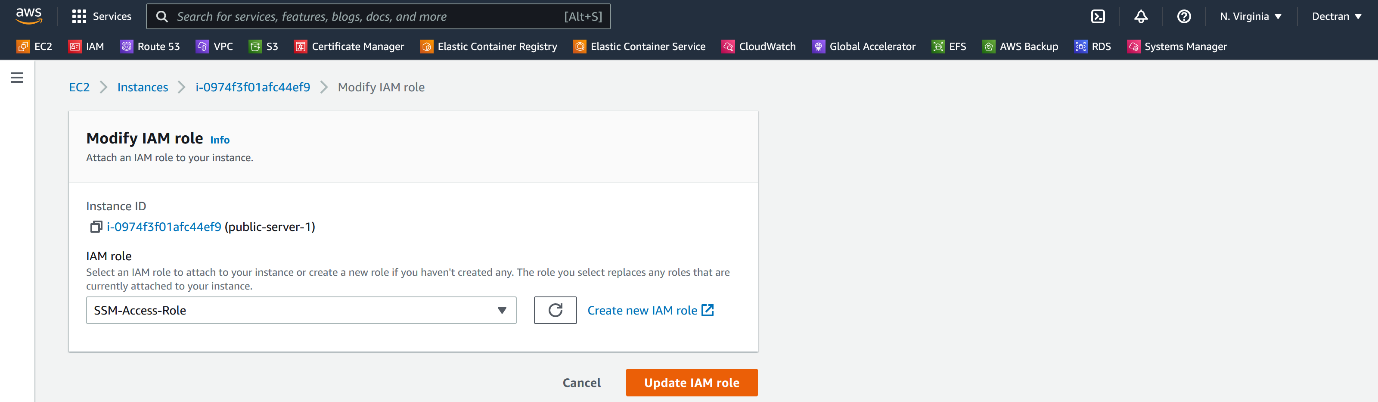
**Attach SSM Access role to instance**



--- I have lost the key for above instance.



--- click on modify IAM Role.



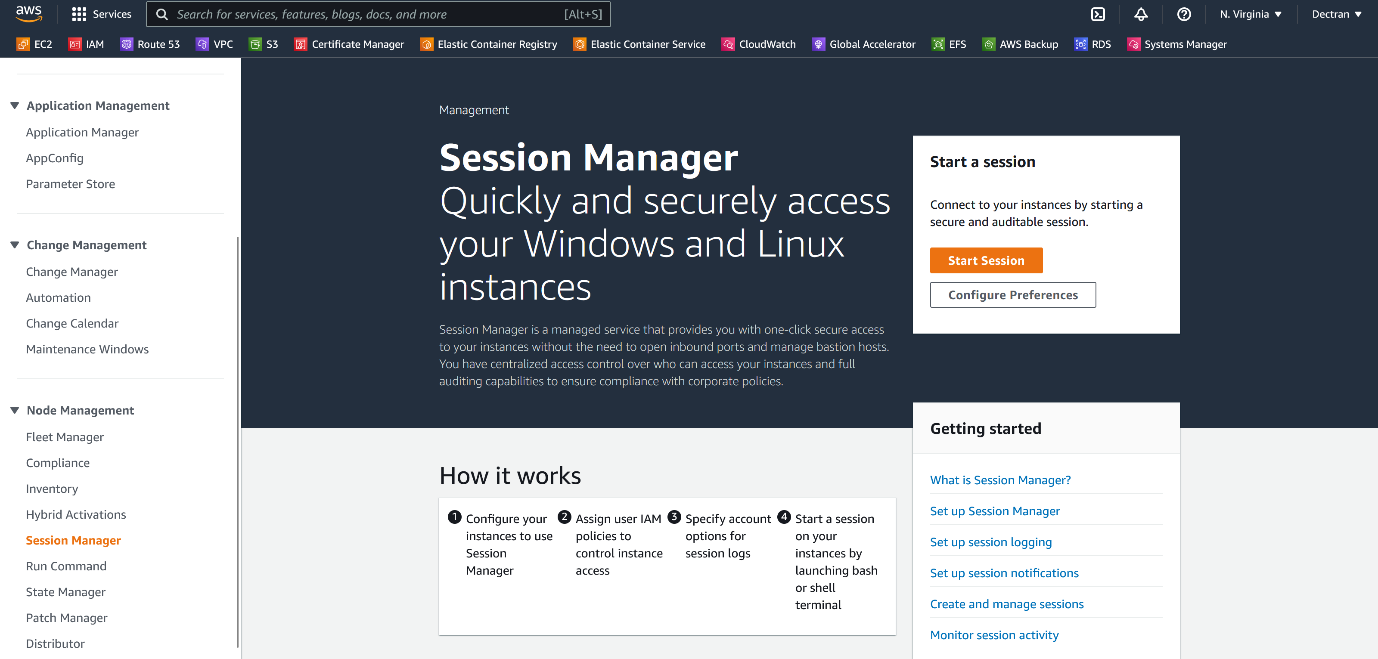
--- click on update IAM role.

--- **important** – Reboot the instance.

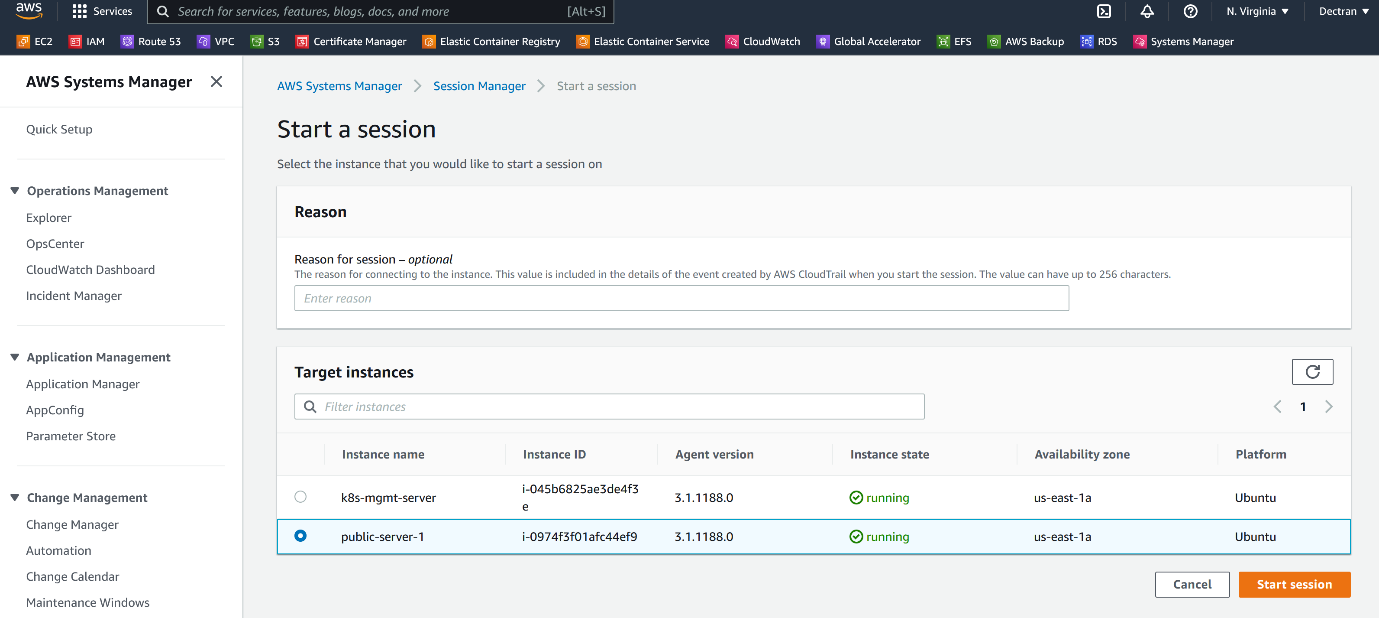
**System manager**

--- go to system manager.

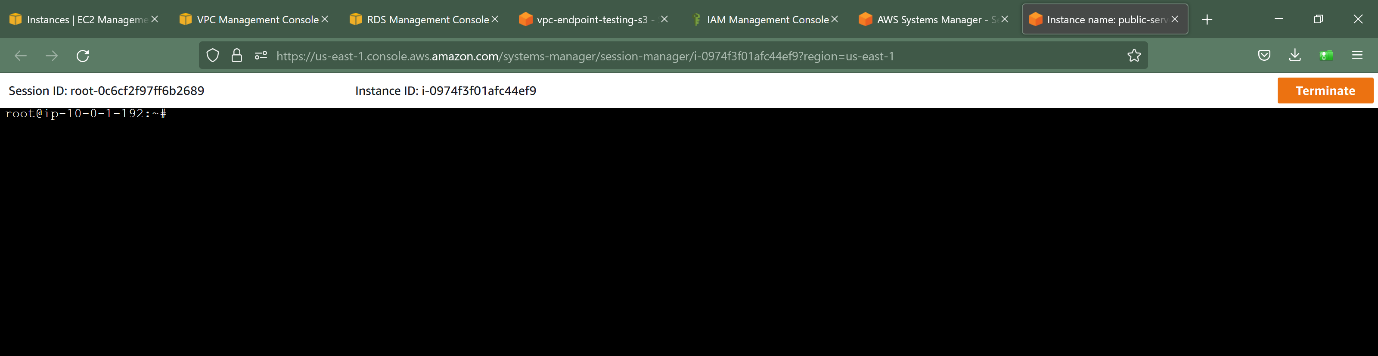
--- click on **session manager**.



--- click on start session.



--- **note** - select our public-server-1 here and click on start session.



--- it will open a window like this, use below commands to enable password authentication.

**# To change into ssm user**

--- bash

**# Change into root user**

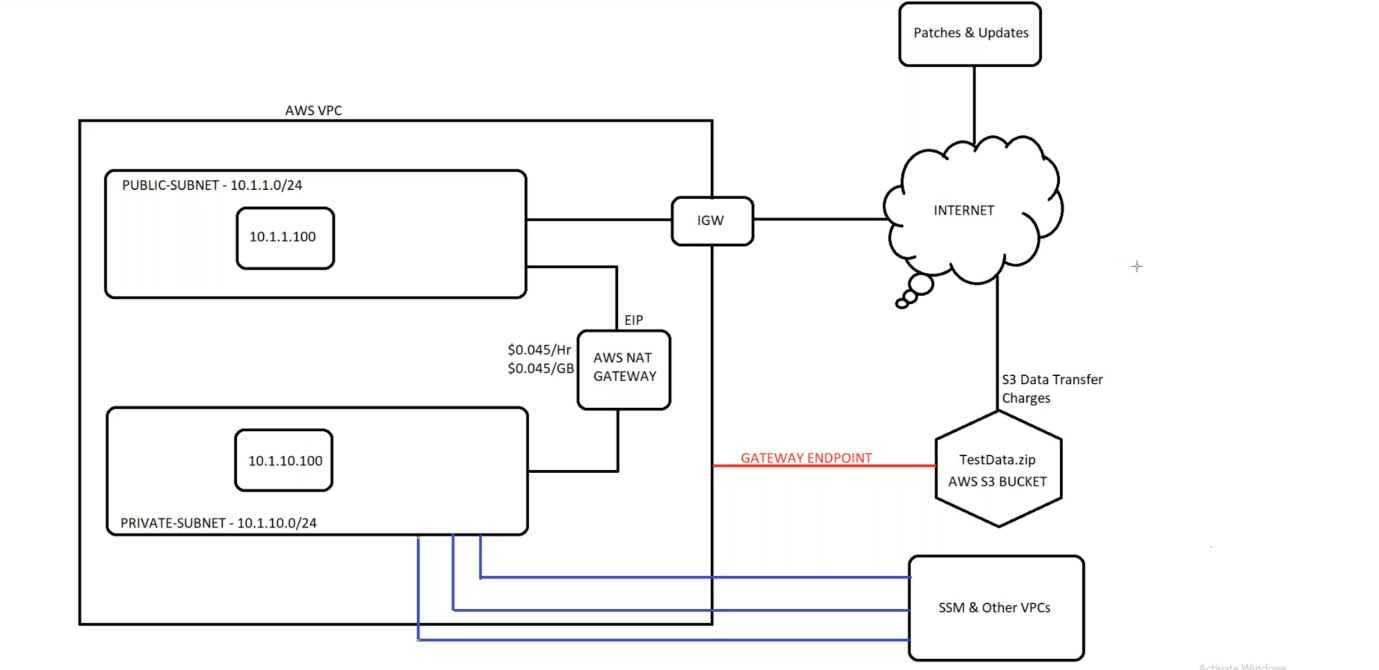
--- sudo su –

**# Enable password authentication**

--- vi /etc/ssh/sshd\_config

--- **note** – now create a user and password, now we can able to login using that user and password.

**Login to private server**



--- **note** – I have lost keys for private instance, how can I connect to this private instance now.

--- **prerequisites**

1. Create 3 endpoins
2. **ec2message endpoints**
3. **ssm endpoints**
4. **ssmmessages endpoints**
5. attach SSM-Access-Role to private instance.

--- **note** – we need to create 3 endpoints to connect a private instance using session manager.

**Session manager**

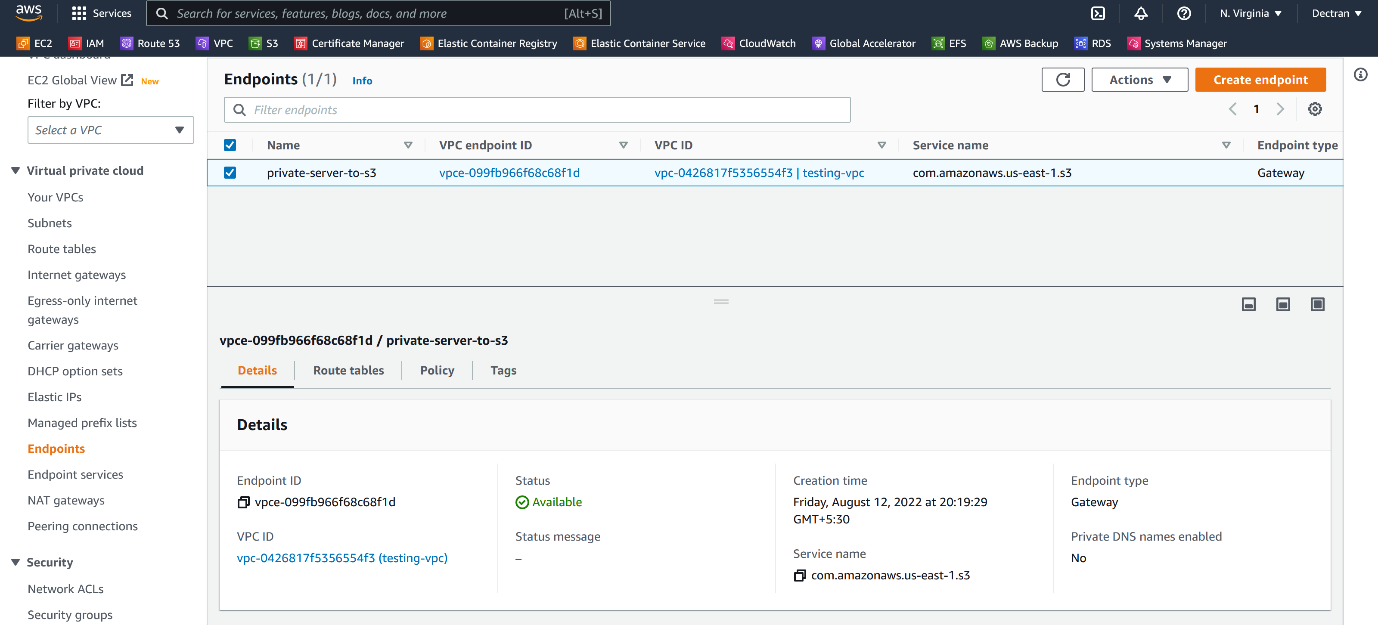
--- go to system manager and now go to session manager.



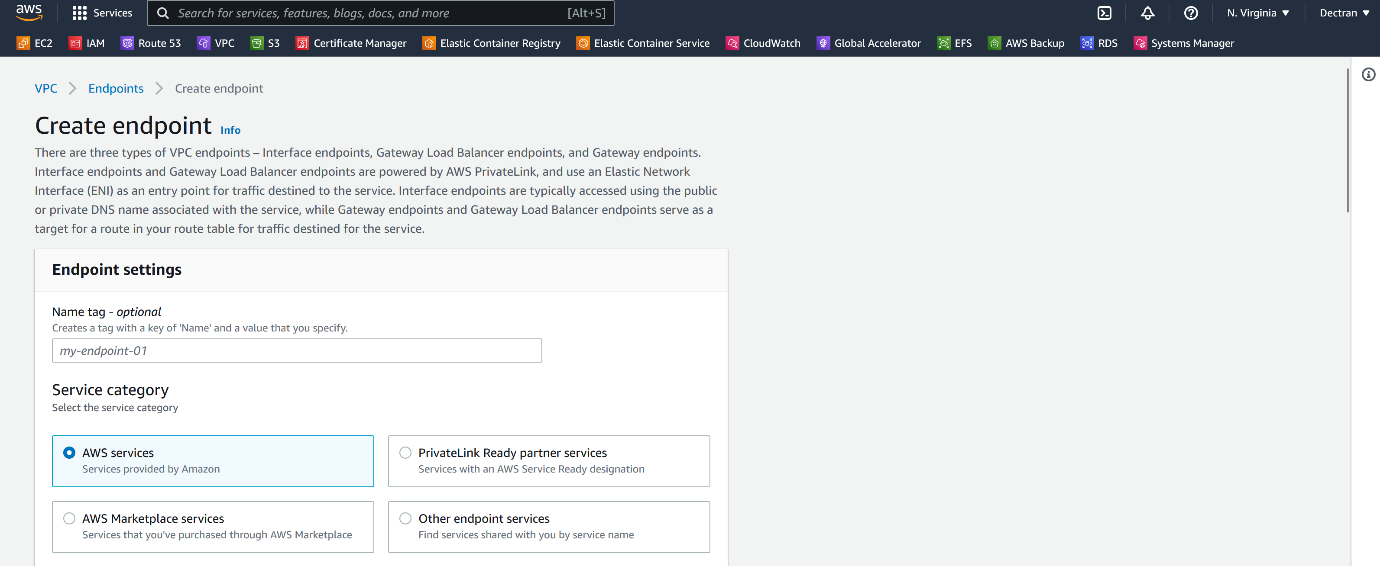
--- **note** – still, we are not able to see our private server here.

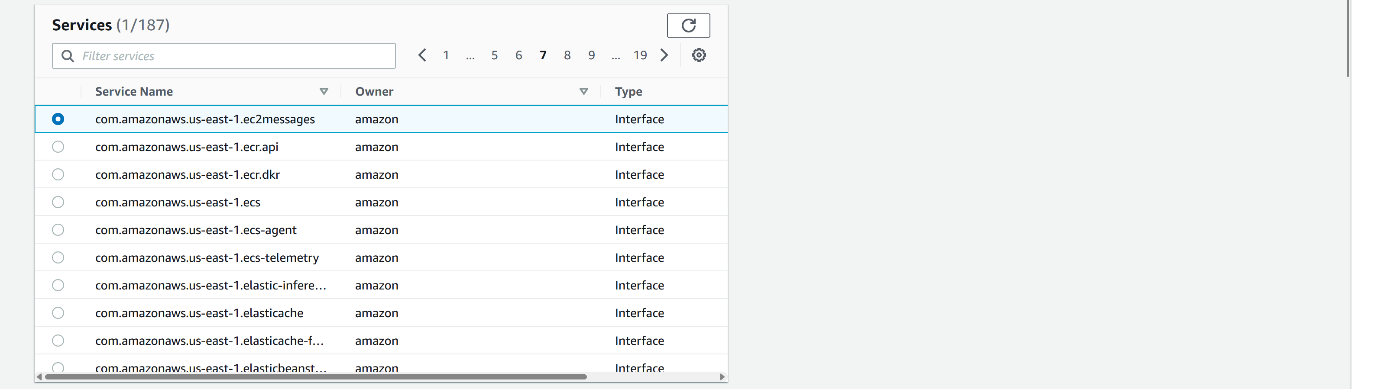
**Create ec2message endpoints**

--- go to vpc and click on endpoints.

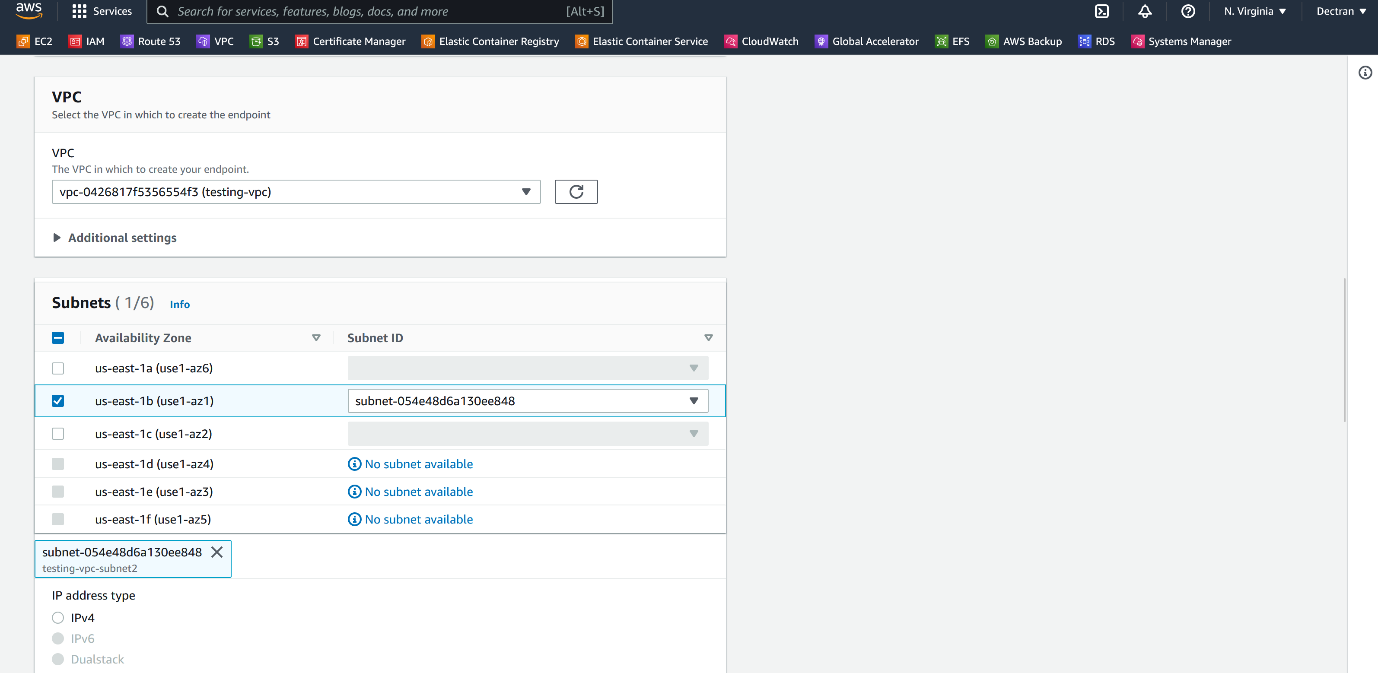


--- click on create endpoint.

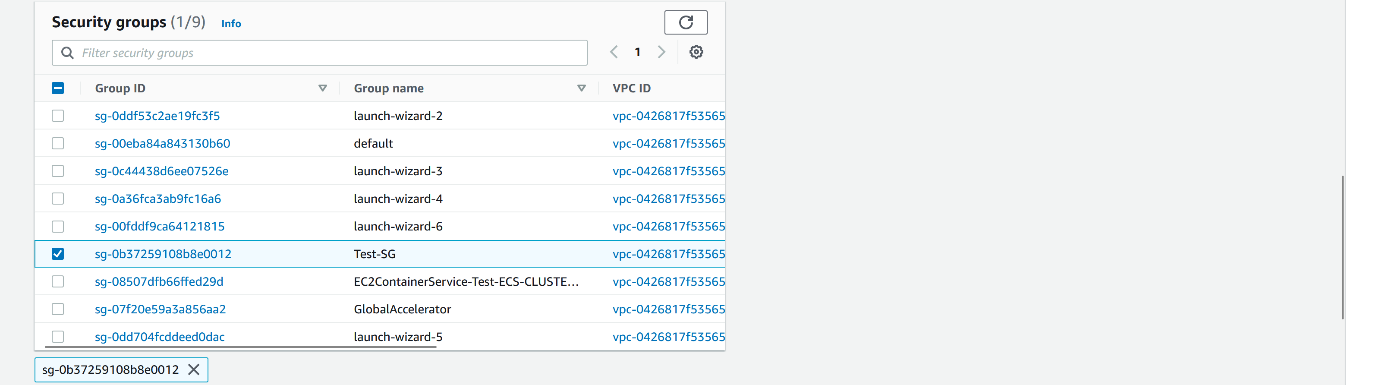




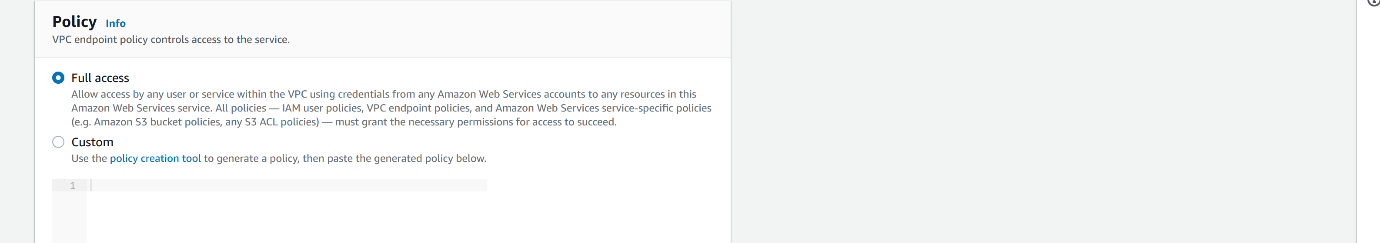
--- select this service - **com.amazonaws.us-east-1.ec2messages**

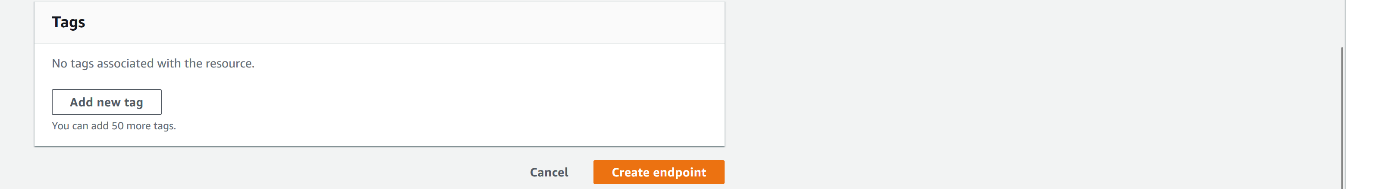


--- select the vpc and private subnet that your private instance in.

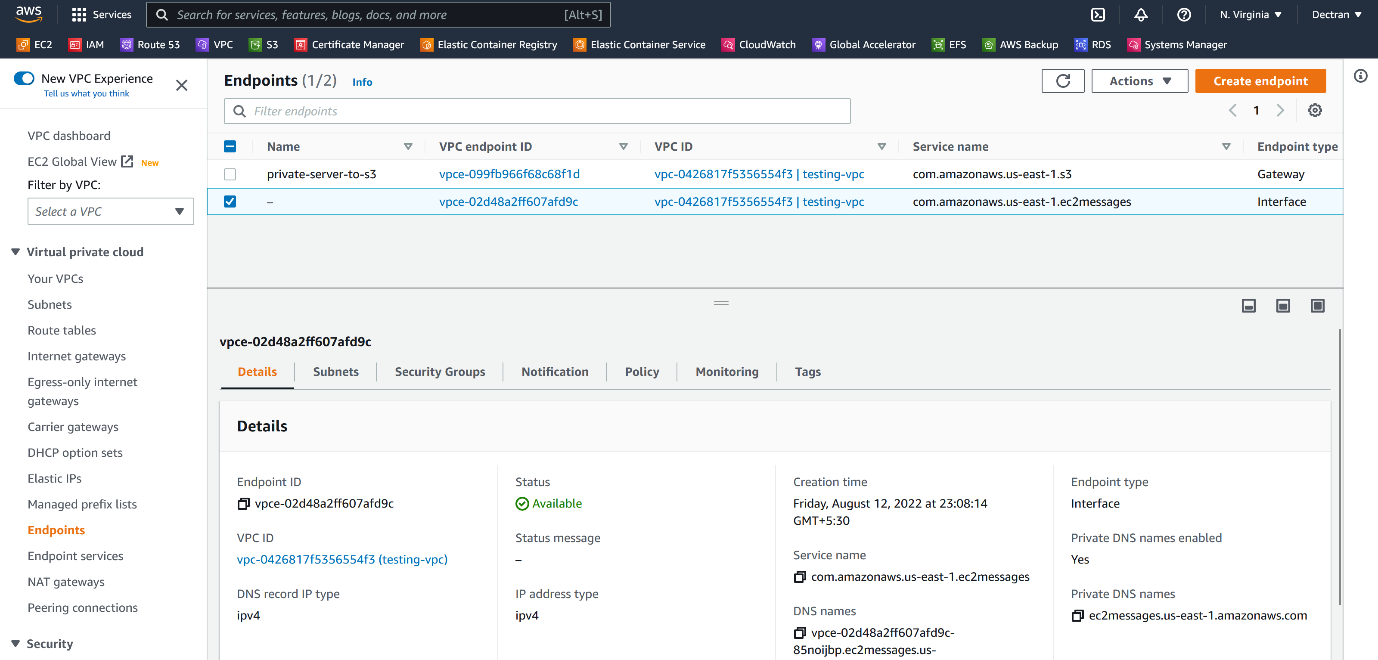


--- in the security group, I am allowing everything.





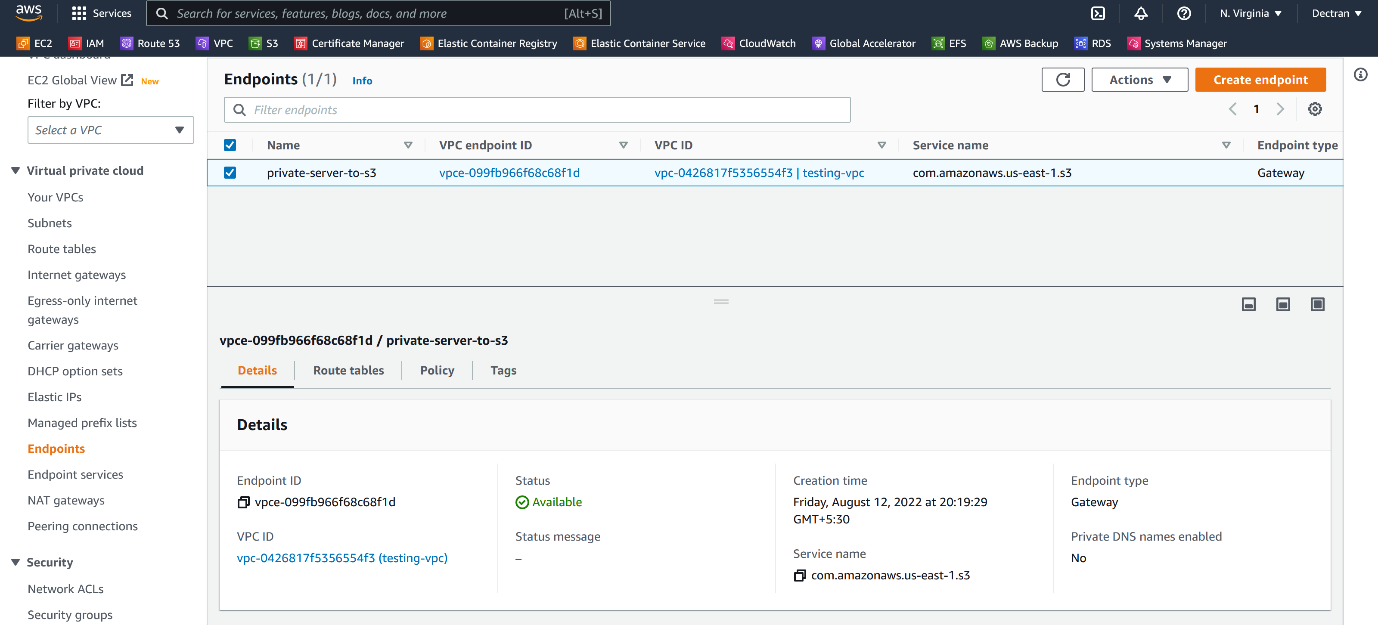
--- click on create endpoints.



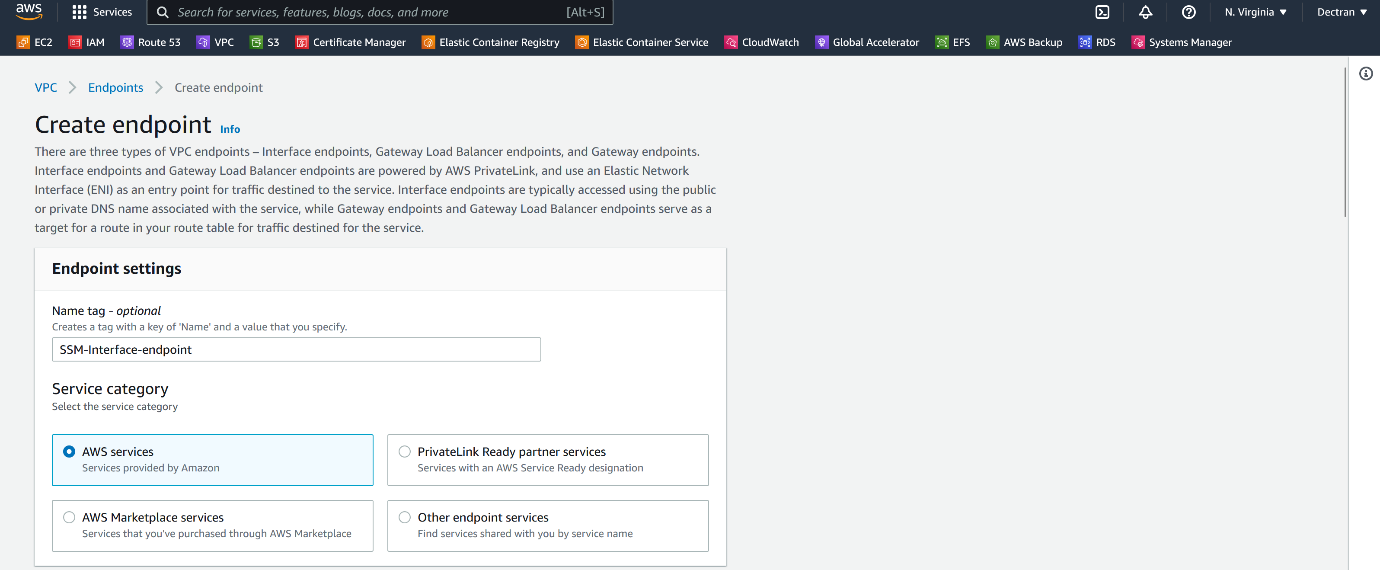
--- endpoint got created.

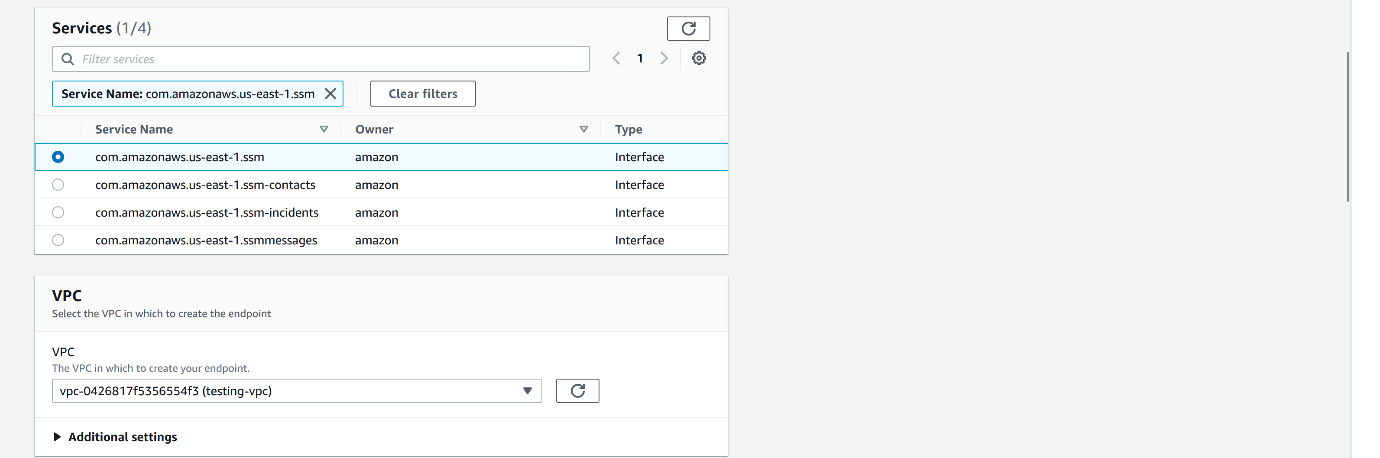
**Create ssm endpoints**

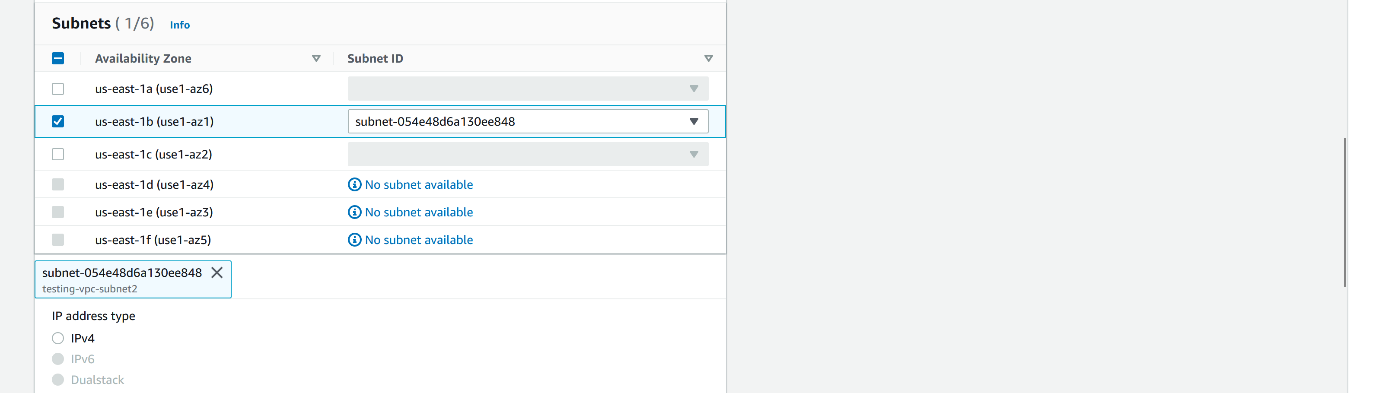
--- go to vpc and click on endpoints.



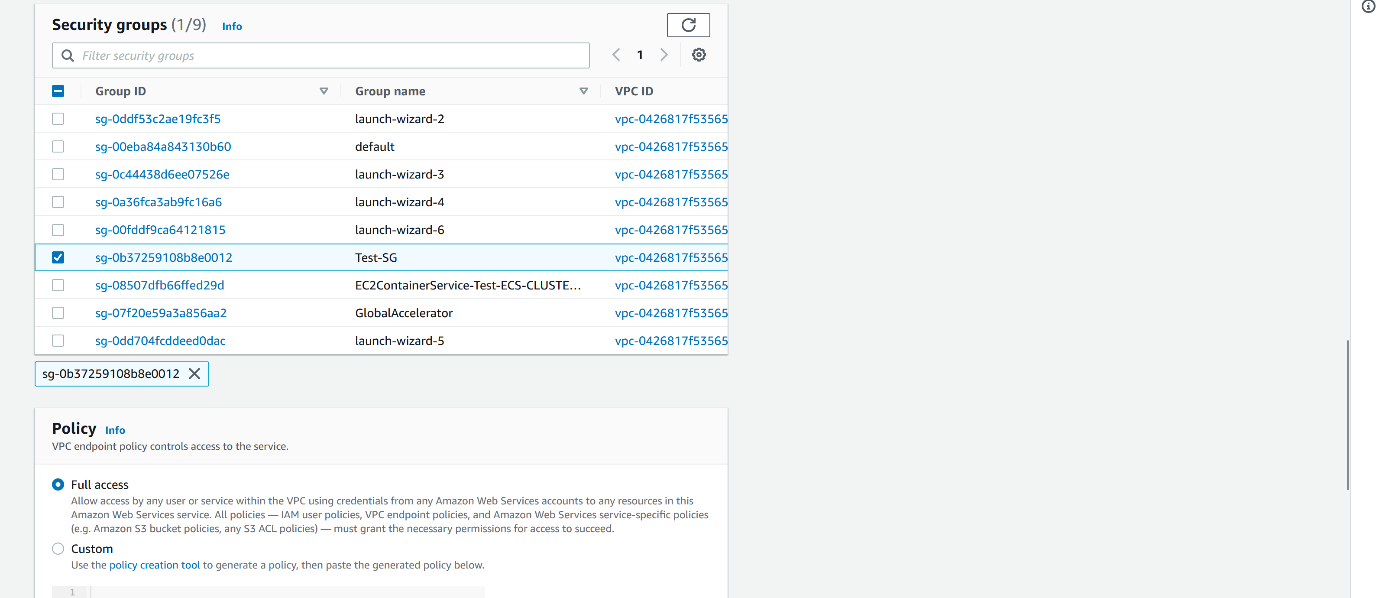
--- click on create endpoint.

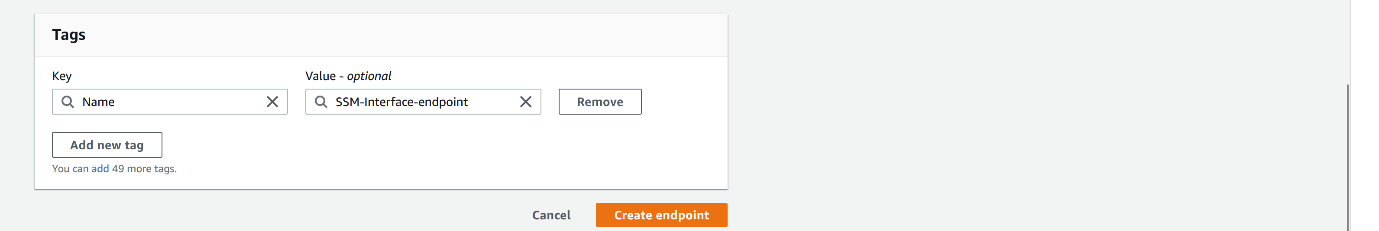




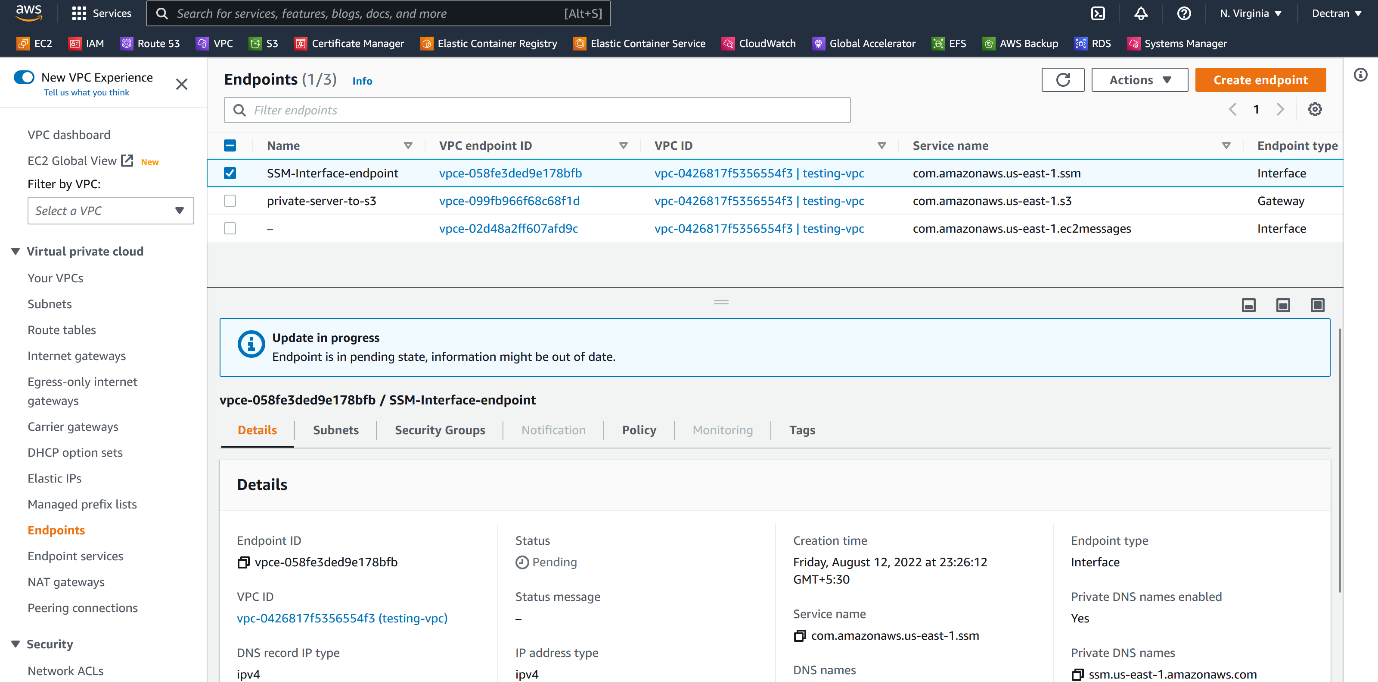


--- select private subnet here.





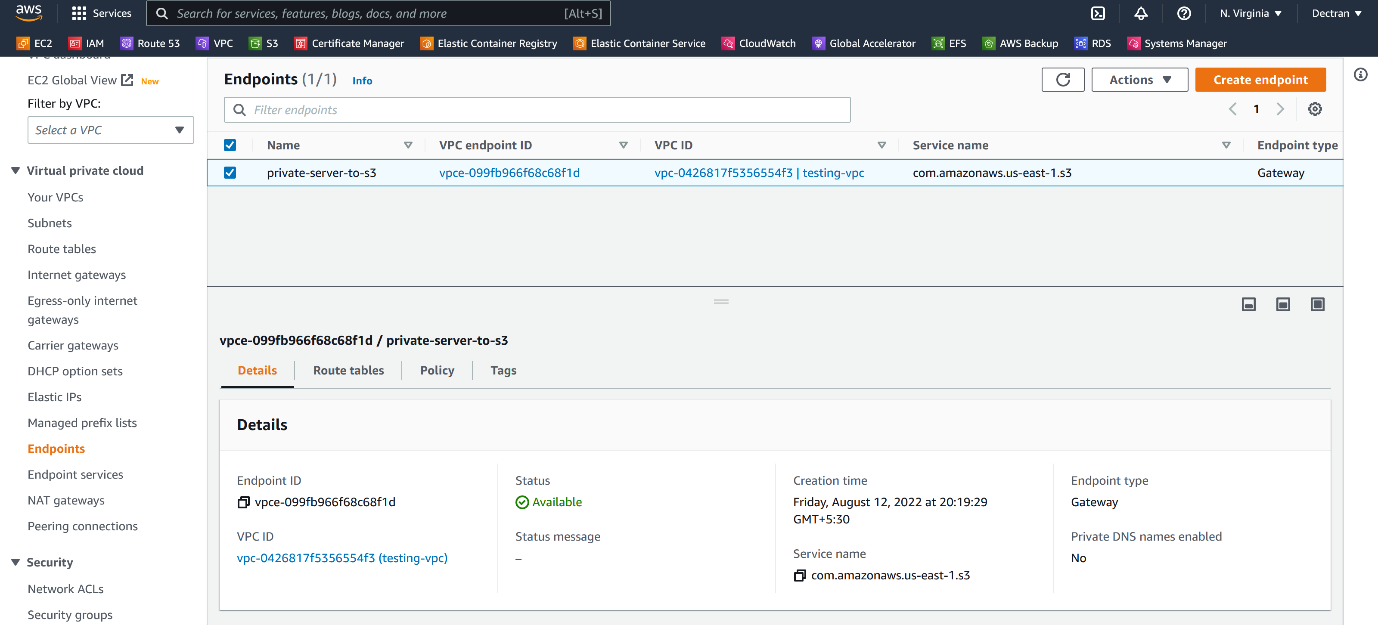
--- click on create endpoint.



--- our SSM interface endpoint got created.

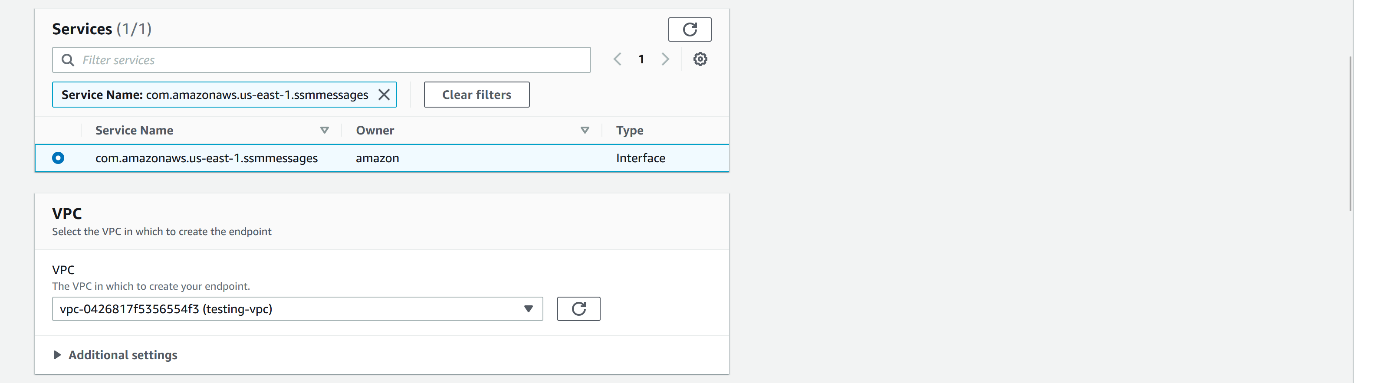
**Create ssmmessages endpoints**

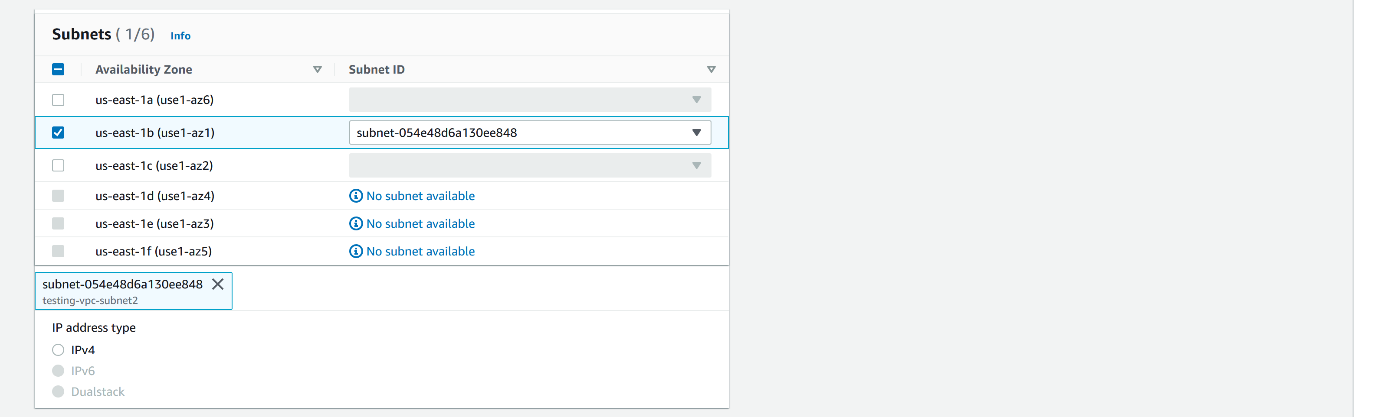
--- go to vpc and click on endpoints.



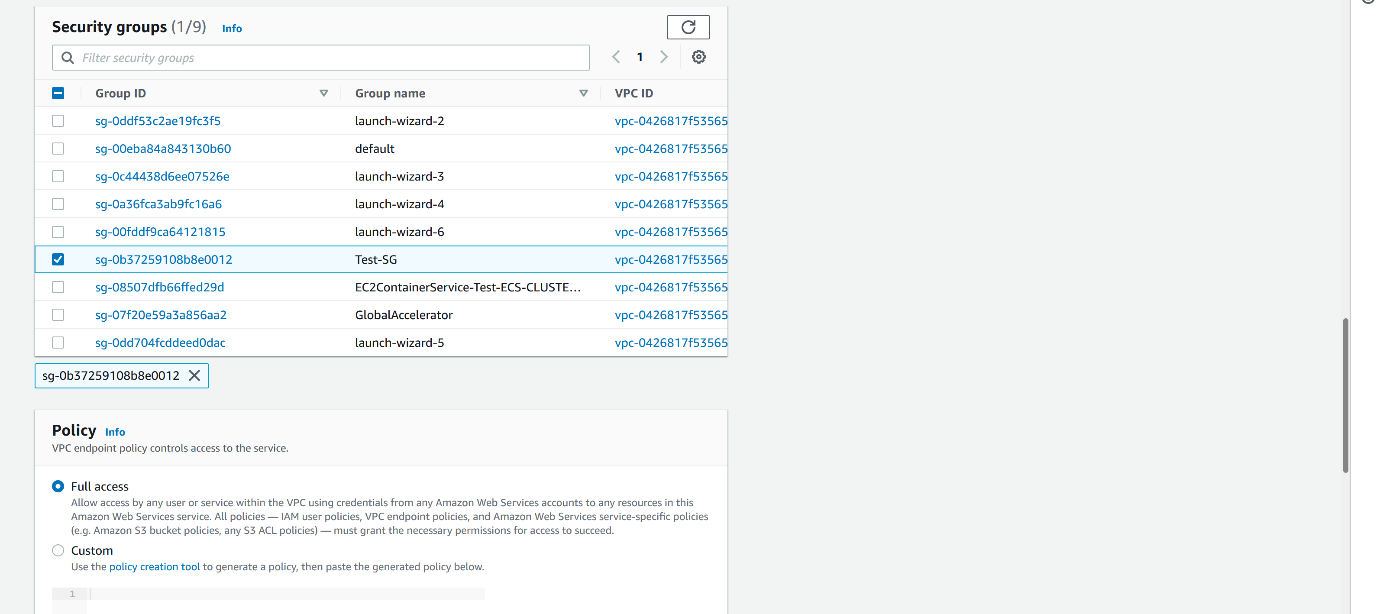
--- click on create endpoint.

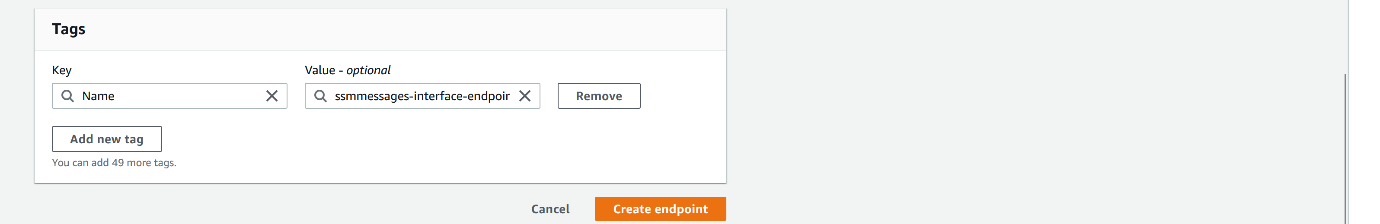




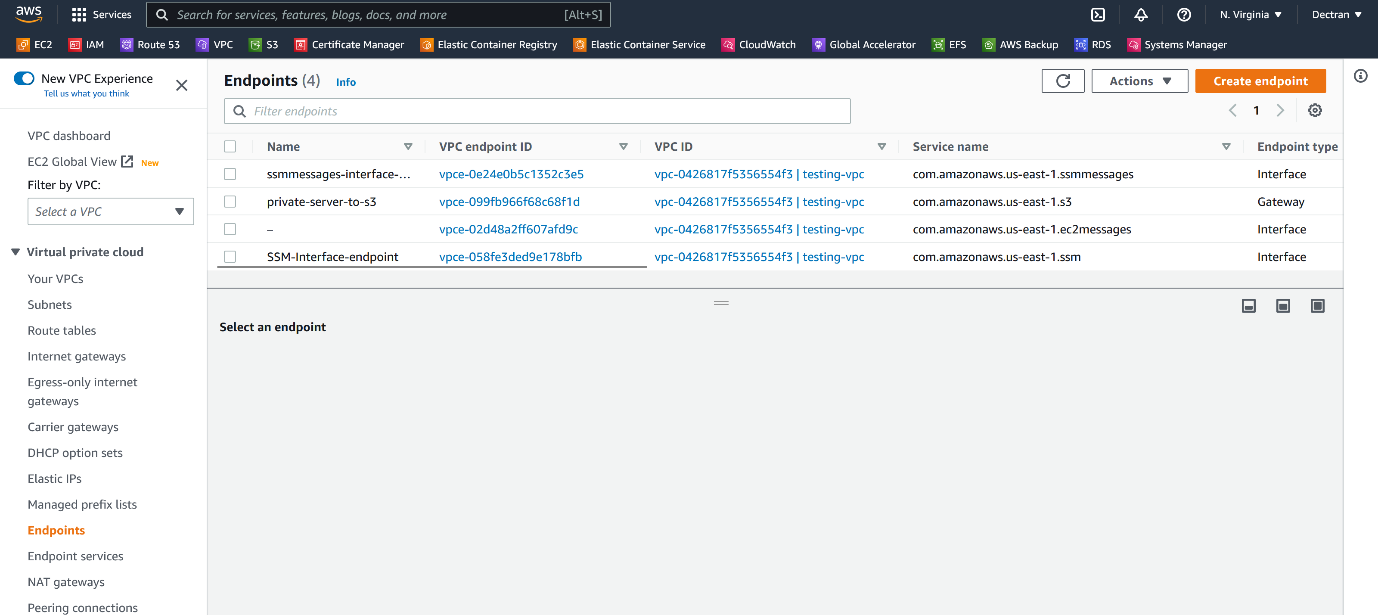


--- select our private subnet.



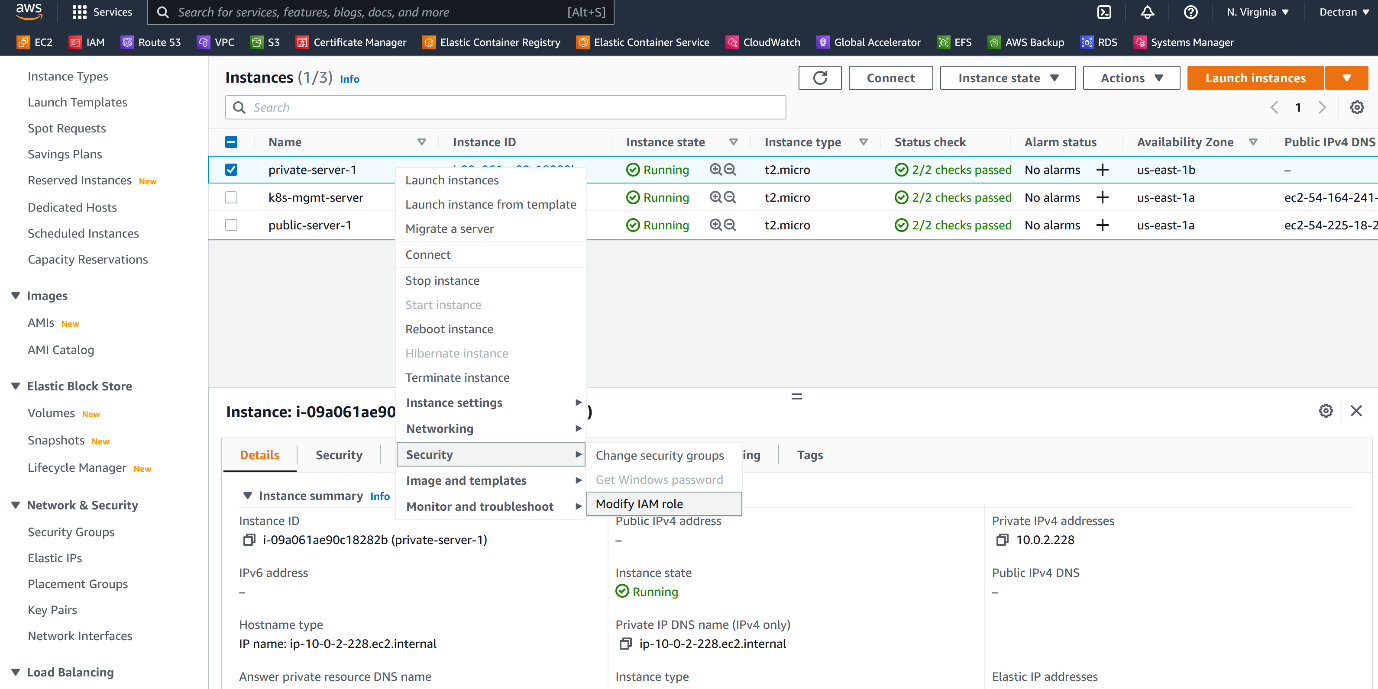


--- click on create endpoint.

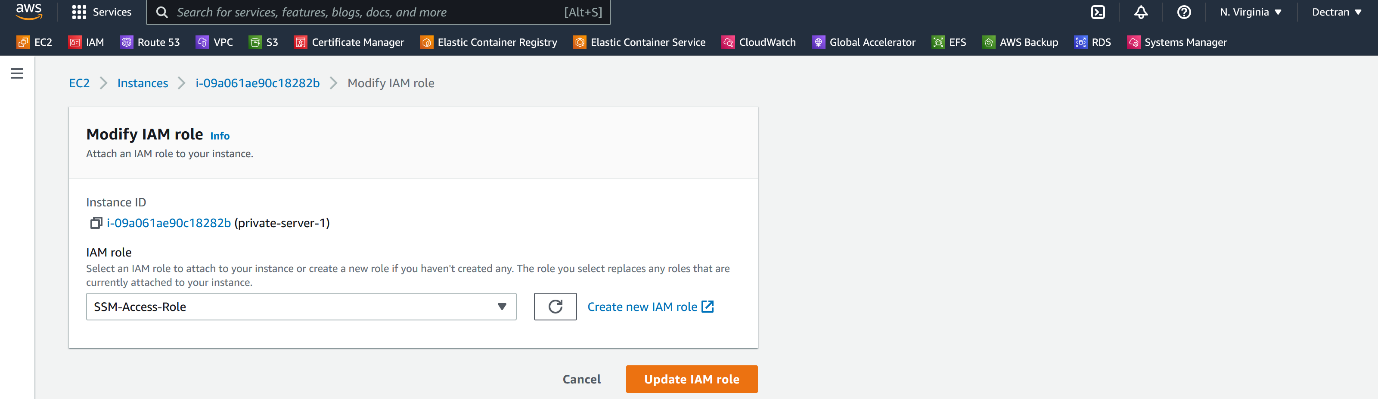


--- our ssmmessages-interface endpoint got created.

**Attach SSM Access role to private instance**

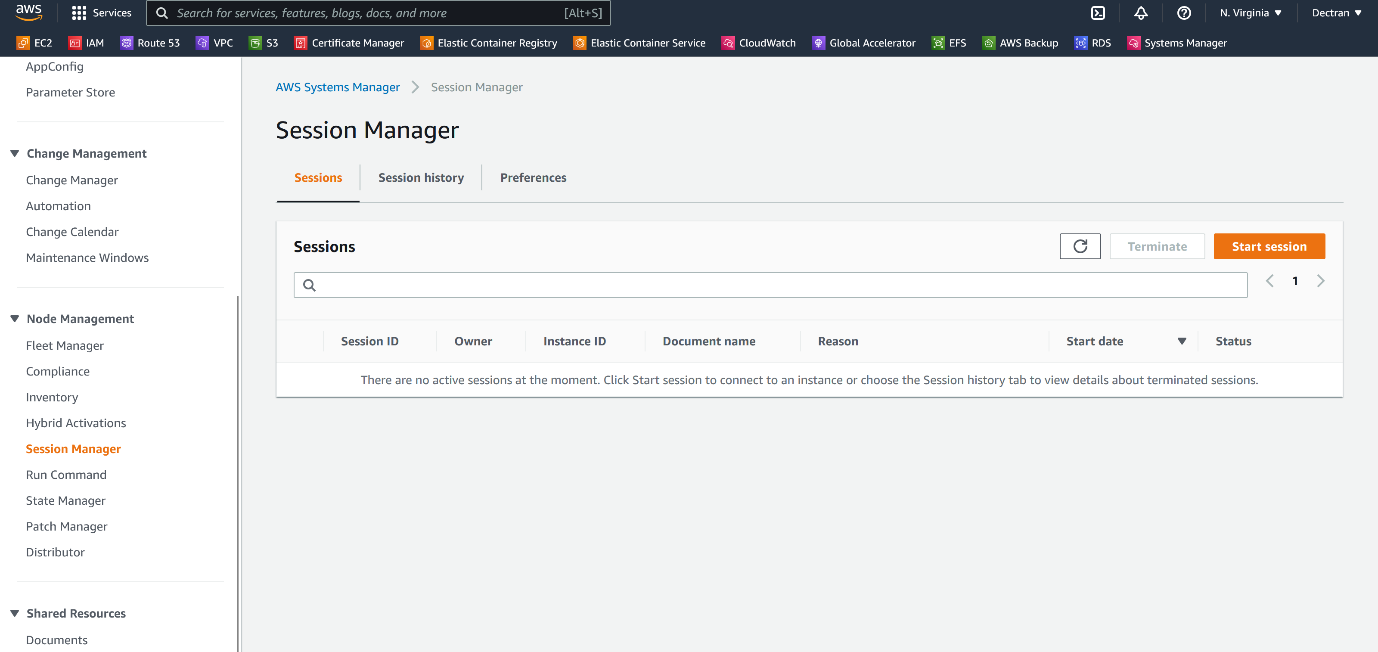


--- click on modify IAM Role.



**System manager**

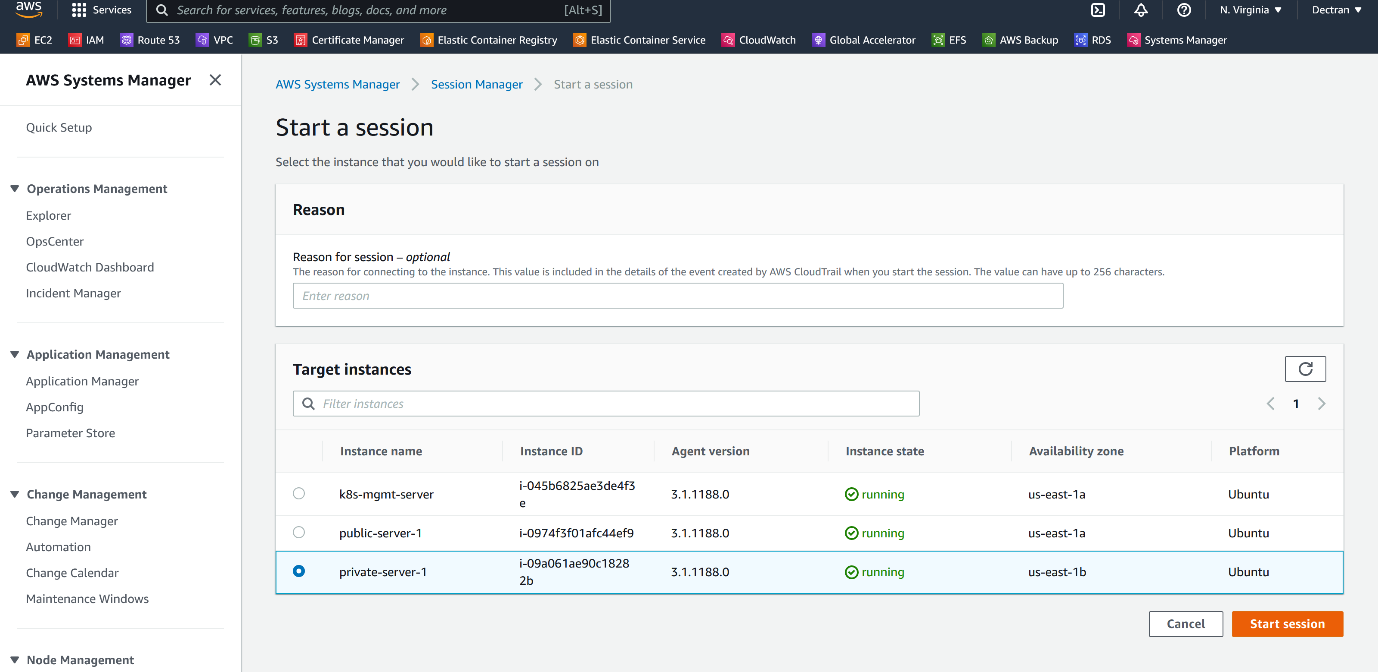
--- select session manager.



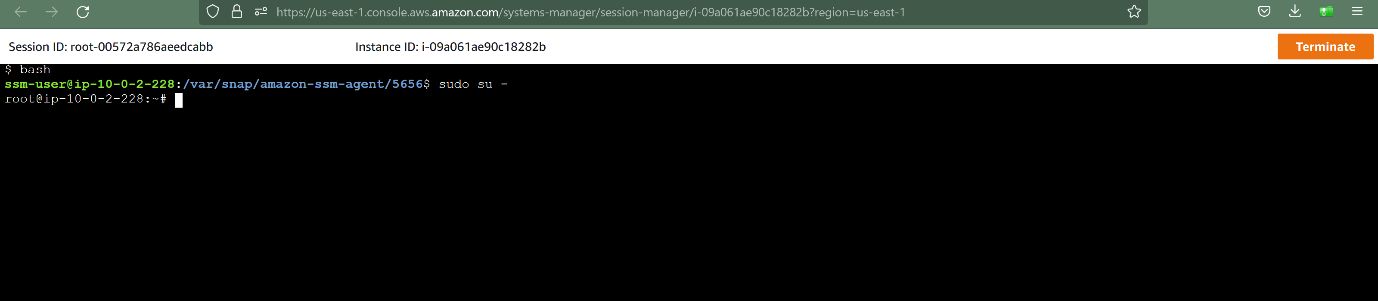
--- **important** – before clicking on start session, reboot private instance. Then only you can see the private instance in the session manager.

--- **note** – reboot is optional, if you wait for 5 to 10min then you can see the private instance in session manager.

--- click on start session.



--- select the private instance and start a new session.



--- it will open a window like this, use below commands to enable password authentication.

**# To change into ssm user**

--- bash

**# Change into root user**

--- sudo su –

**# Enable password authentication**

--- vi /etc/ssh/sshd\_config

--- **note** – now create a user and password, now we can able to login using that user and password.