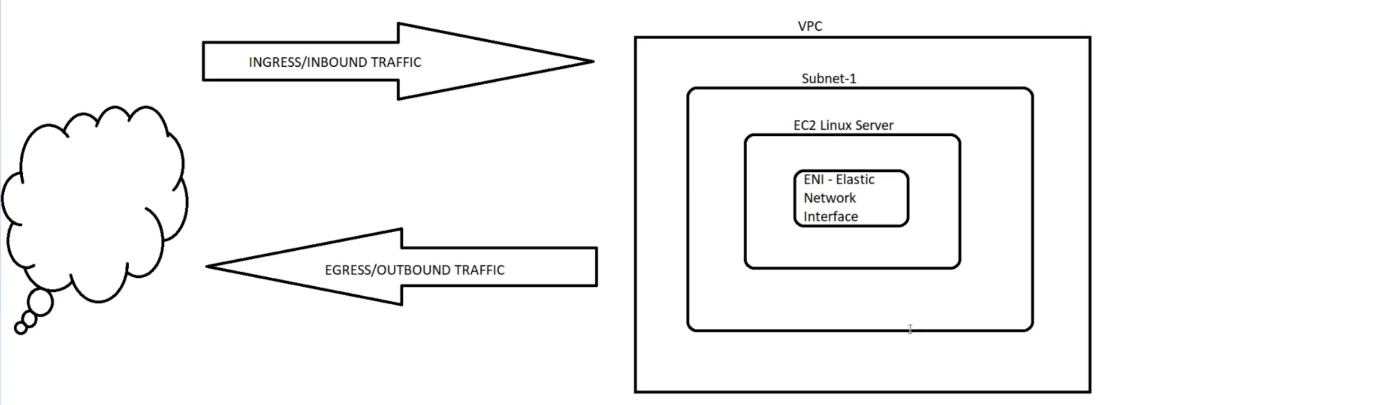
**08.AWS-B30-Flowlogs-FirewallOverview-ActiveDirectoryDeployment**

--- we will discuss about below topics

1. VPC flow logs
2. DHCP options
3. Egress gateway

**VPC Flow logs**



--- **How do you monitory the traffic in VPC…?**

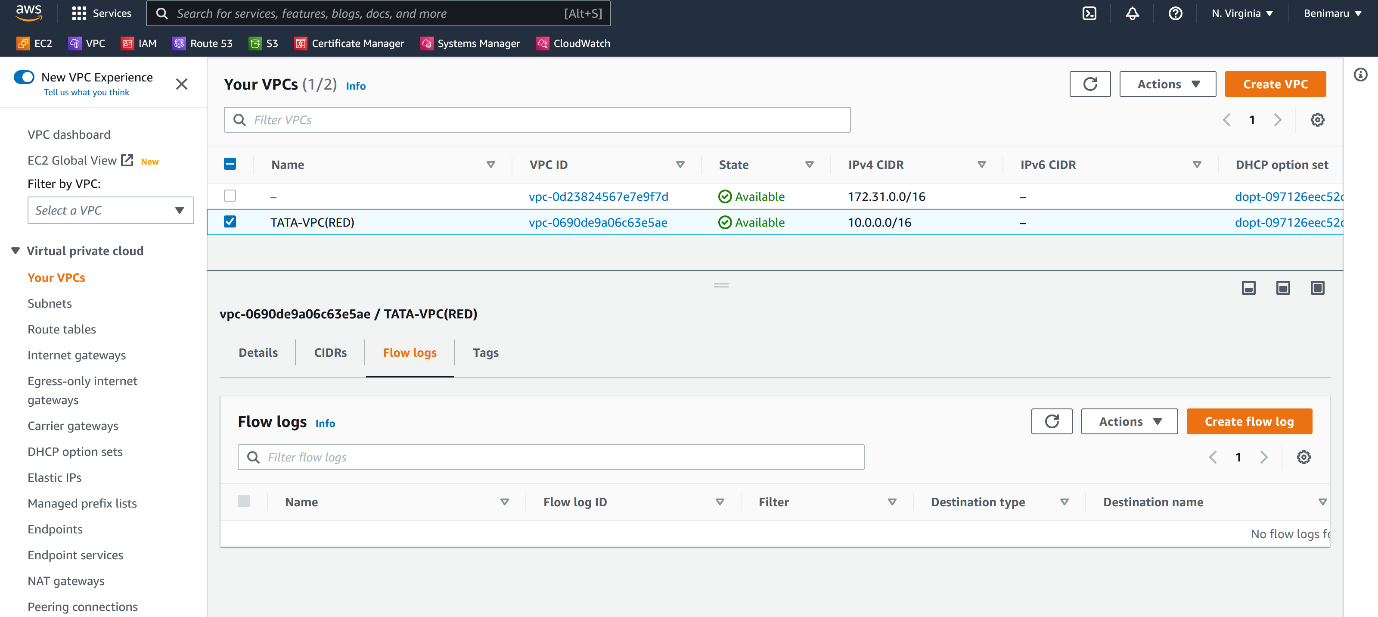
Using VPC flow log, inbound and outbound traffic logs can be enabled on VPC using VPC Flow logs. All the

--- if you enable vpc flow log on vpc then it will automatically applicable to all the subnets which are present inside of vpc and it is also applicable on EC2 instance also.

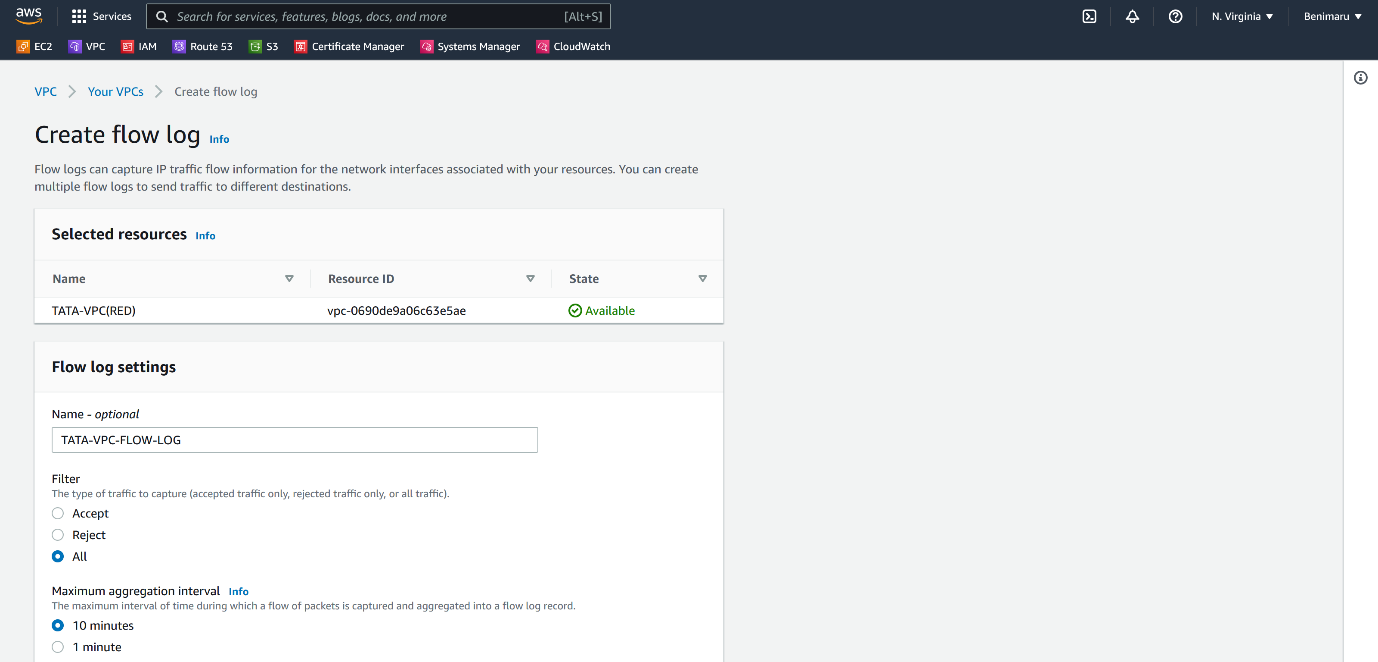
--- enabling VPC flow log on VPC is very dangerous because if you have 1000 of servers then all the activity of the servers will be monitored.

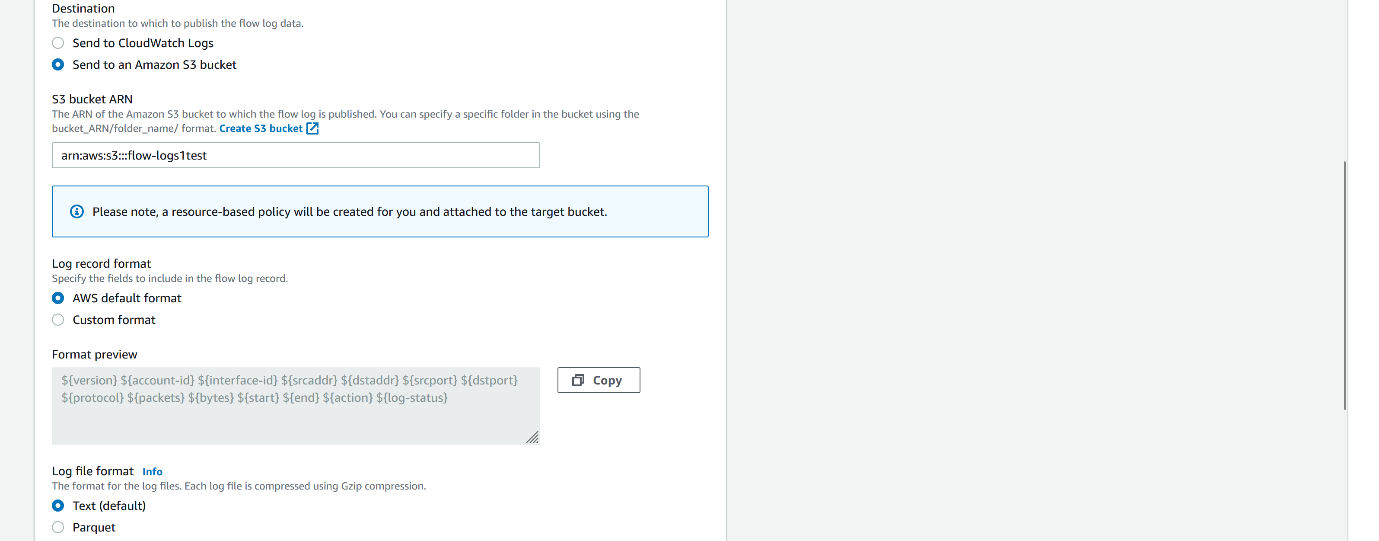
**Create VPC flow log**

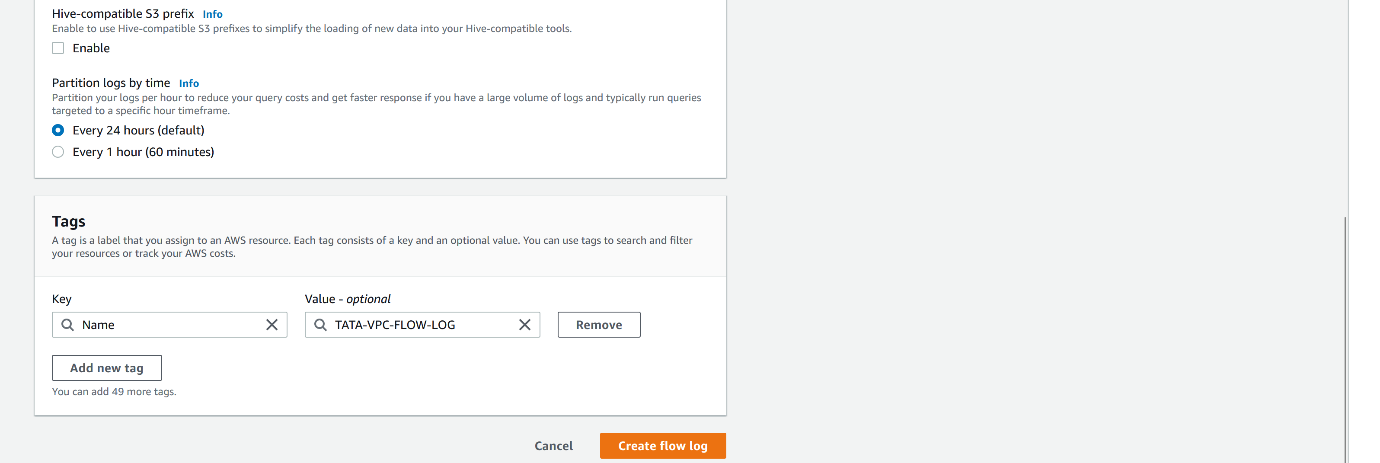
--- go to the VPC.



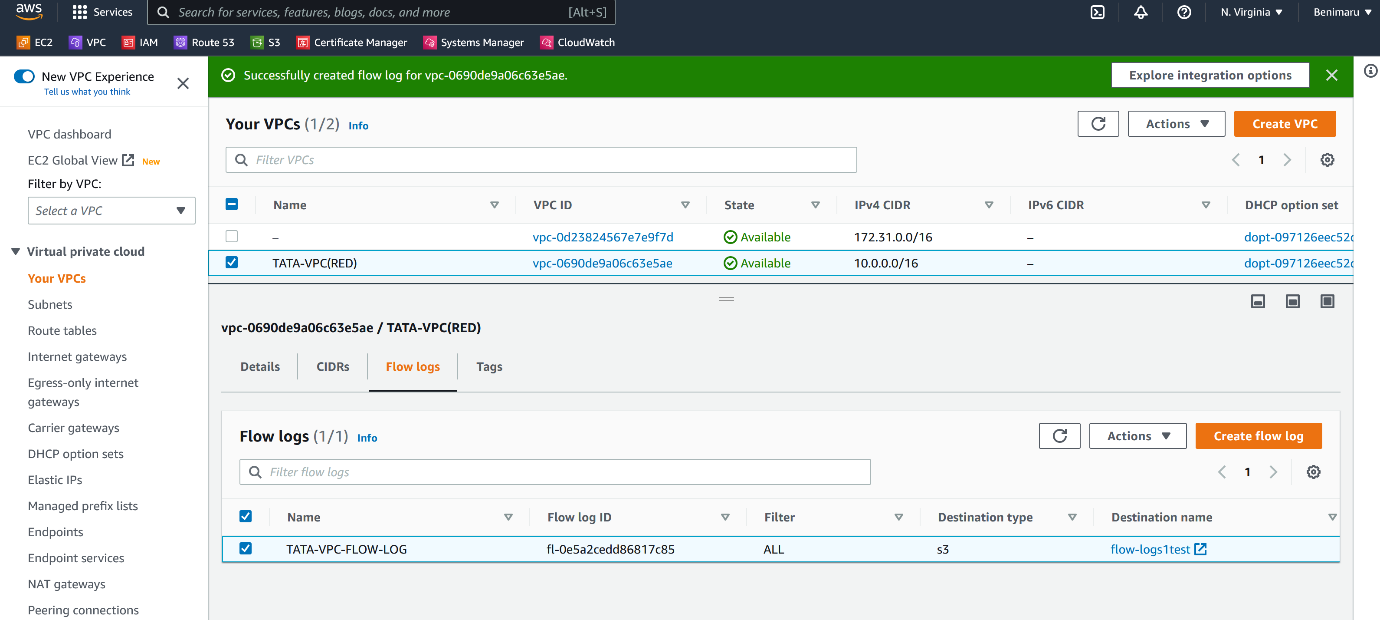
--- Click on create flow log.







--- click on create flow log.



--- VPC flow log is enabled on our VPC.

**Egress only internet gateways**

--- **note** – if you are using ipv6 ip address then we will use egress only internet gateways.

--- here there is no public and private ips. All the ips here is public ips

**State full and state less firewall**

--- **security group** - state full firewall.

--- **NACL** – State less firewall.

**State full firewall**

--- **note** – if you open port in inbound then you do not need to open the port in outbound.

Eg security group. Applied to EC2, RDS, ELB etc.

**Sate less firewall**

--- **note** – you need to open the port in inbound and outbound as well.

Eg NACL – only applied to subnets. We apply outbound to subnets only.