VIRTUAL PRIVATE CLOUD (VPC)

A virtual private cloud (VPC) is a virtual network that closely resembles a traditional network that you'd operate in your own data centre, with the benefits of using the scalable infrastructure of Amazon Web Services (AWS).

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.

You can create isolated networks for your applications or clients.

VPC: A *virtual private cloud* (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings.

Subnet: A *subnet* is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.

Route Table: A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed.
Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Internet Gateway: An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

An Internet gateway serves two purposes: to provide a target in your VPC route tables for Internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IP addresses.

Network ACLs: A *network access control list (ACL)* is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

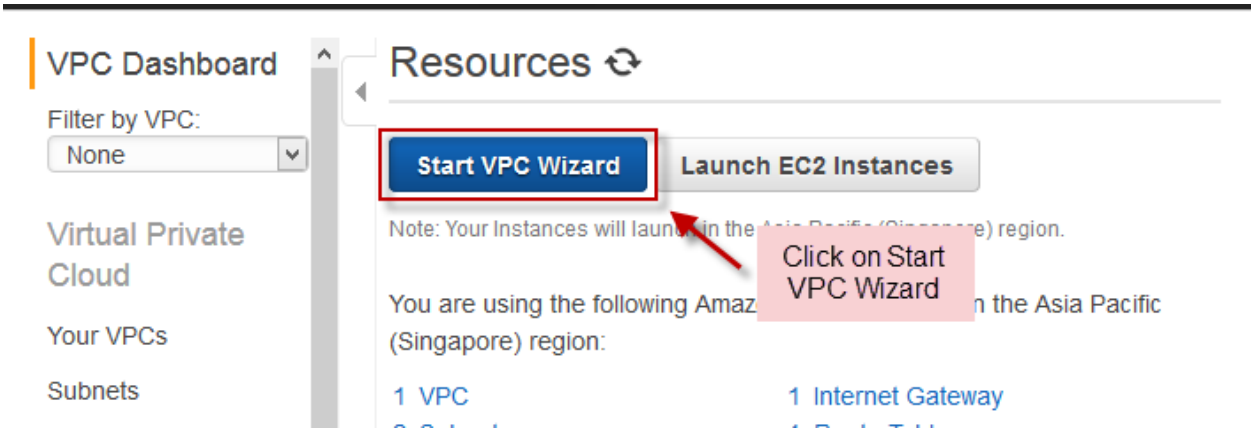
Scenario	Usage
Scenario 1: VPC with a Single Public Subnet	Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet.
Scenario 2: VPC with Public and Private Subnets (NAT)	In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).
Scenario 3: VPC with Public and Private Subnets and Hardware VPN Access	This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your data center - effectively extending your data center to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.
Scenario 4: VPC with a Private Subnet Only and Hardware VPN Access	Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

VPC CONFIGURATION

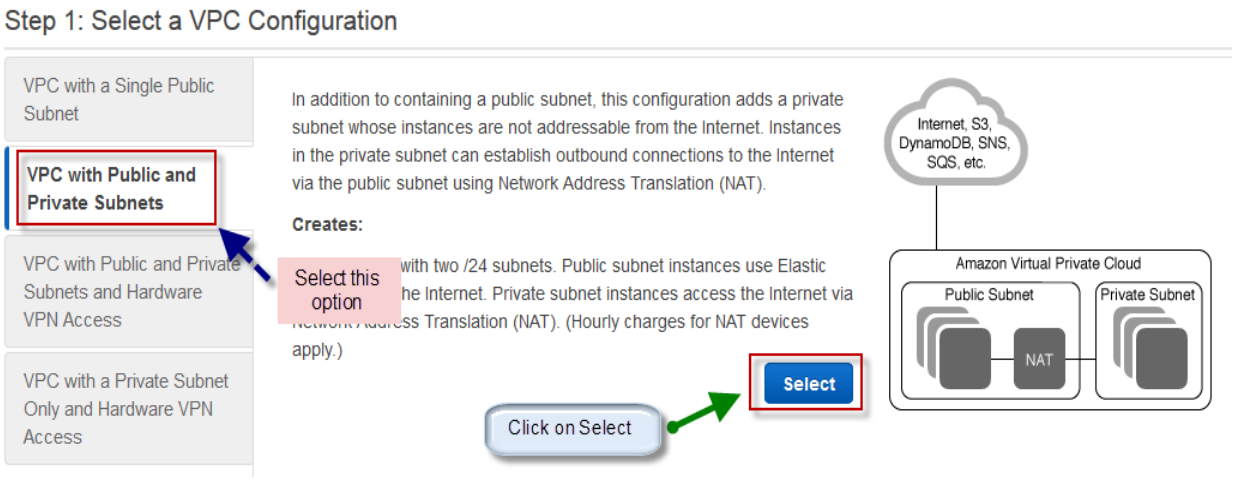
Creating VPC using VPC wizard:

Once you have logged in to AWS, click on VPC under Networking section in AWS console home page.

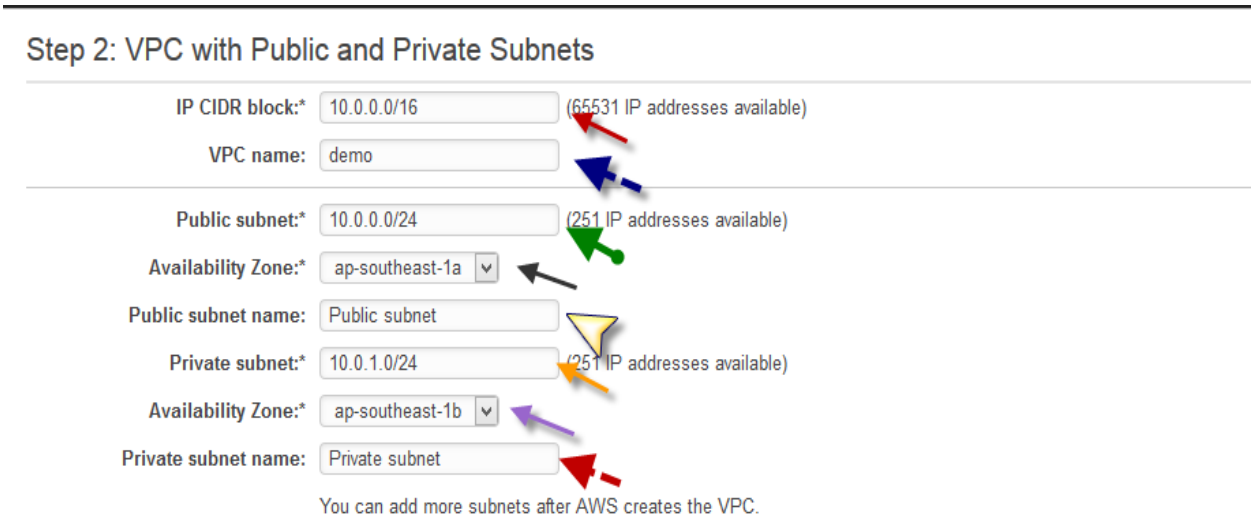
Once you are in VPC dashboard page, click on **Start VPC Wizard.**



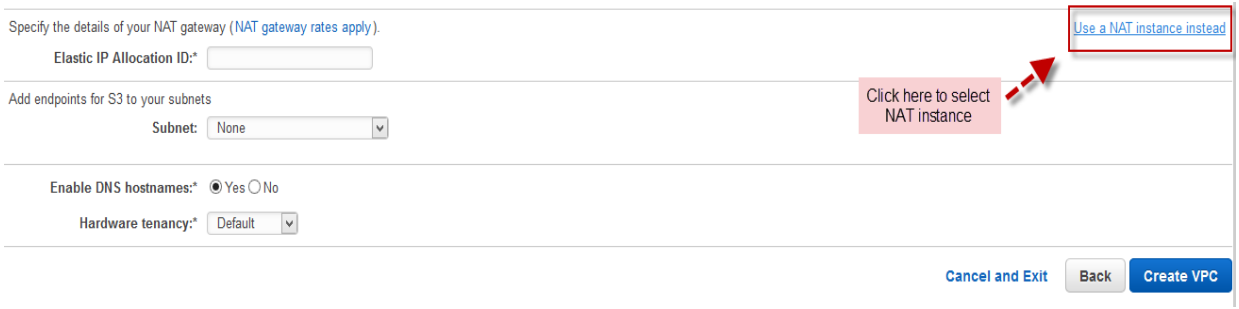
In the next page, select one VPC configuration as per your requirement.
In this example we are selecting **VPC with Public and Private Subnets.**
Once selected, click on Select.



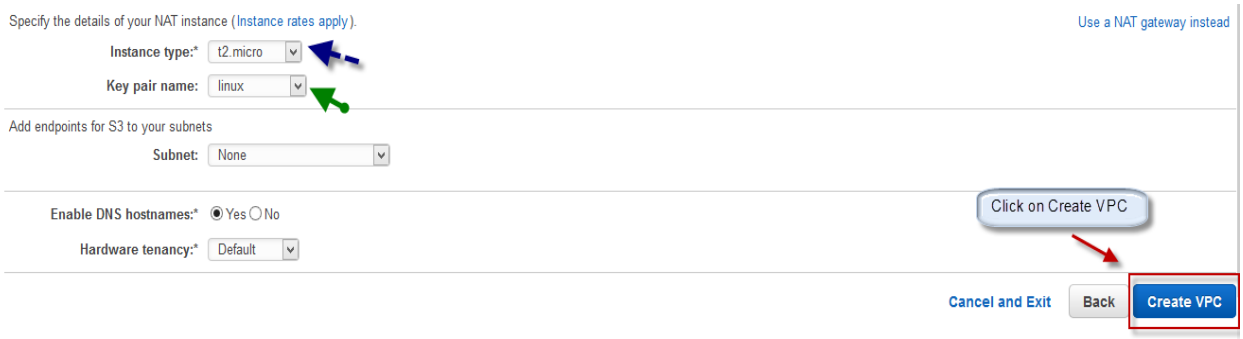
In the next window, specify a IP CIDR block, VPC Name, Specify Public Subnet IP range, select the Availability zone from the drop down list, specify a name for public subnet, specify a IP range for private subnet, availability zone from the drop down list, and specify a name for private subnet.



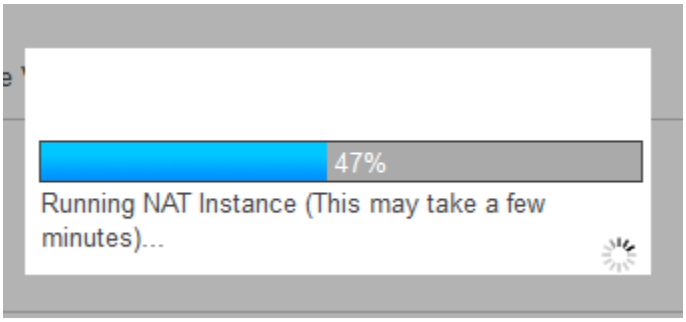
In the middle of the page select **Use a NAT instance instead**.



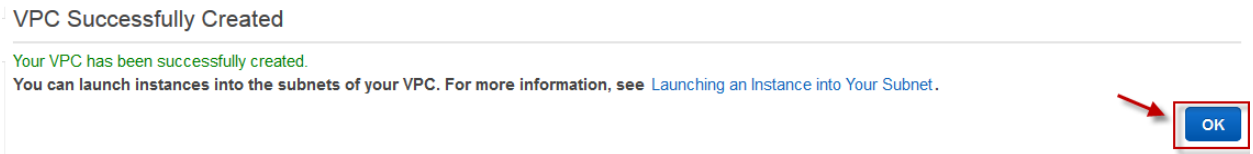
In the below of the page, after clicking Nat instead, select Instance type for NAT and Key pair for NAT instance.
Then leave rest to defaults and click on **Create VPC.**



It will start creating VPC with selected configuration.

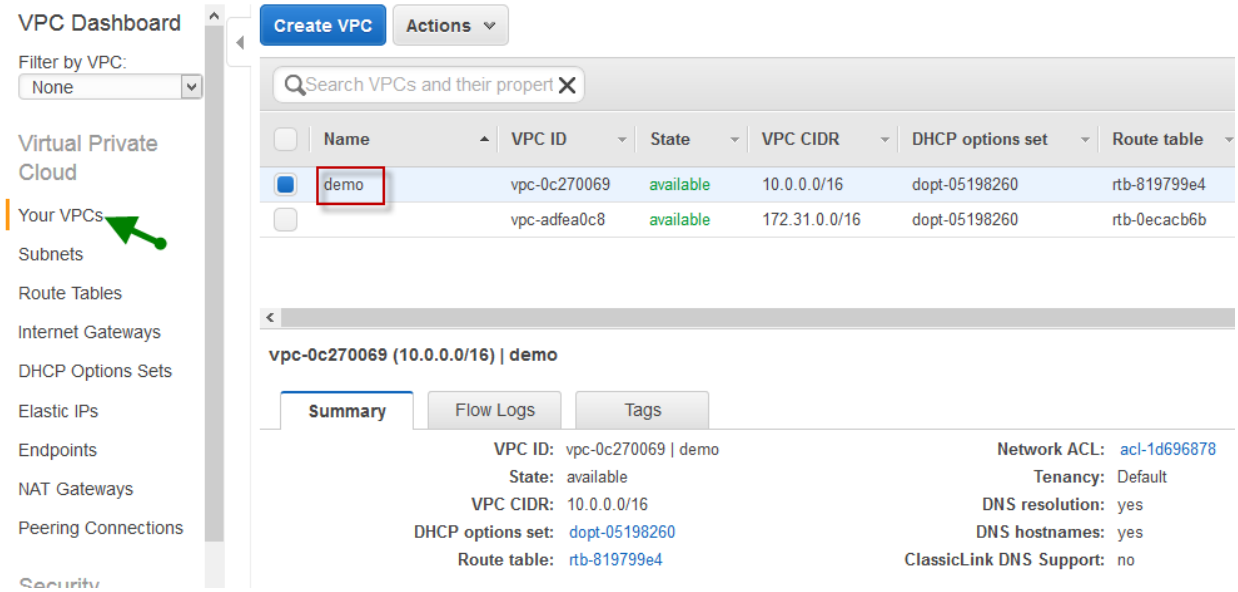


Once created, you will be displaying message on the saying VPC successfully Created, click on OK to continue to access the VPC.



Once completion of VPC creation, go to **Your VPCs** from left pane under VPC dashboard.

You can be able to see the created VPC.



Security in Your VPC

Amazon VPC provides three features that you can use to increase and monitor the security for your VPC:

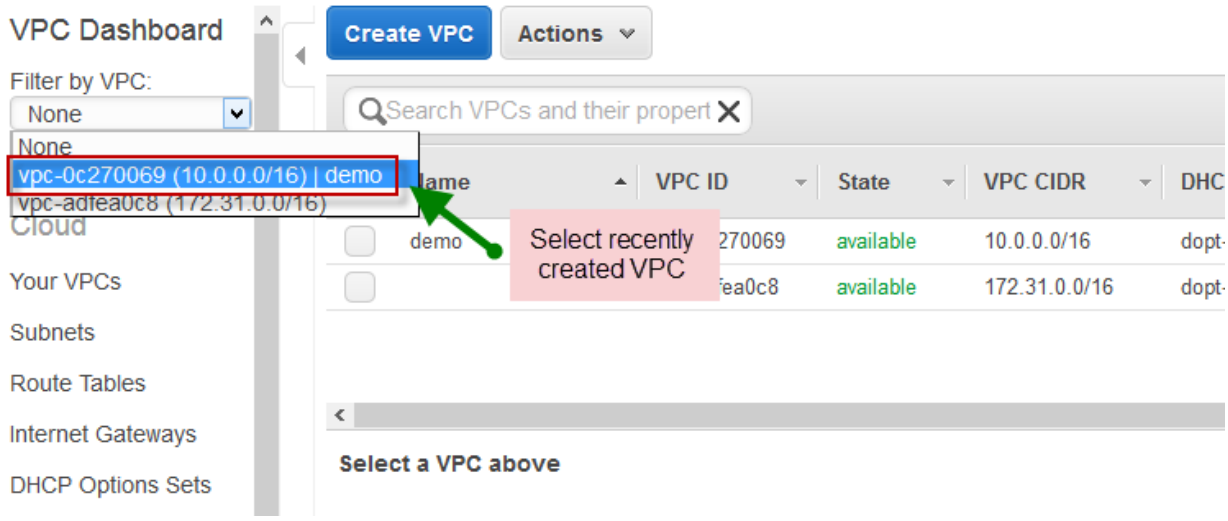
Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level

Network access control lists (ACLs): Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level

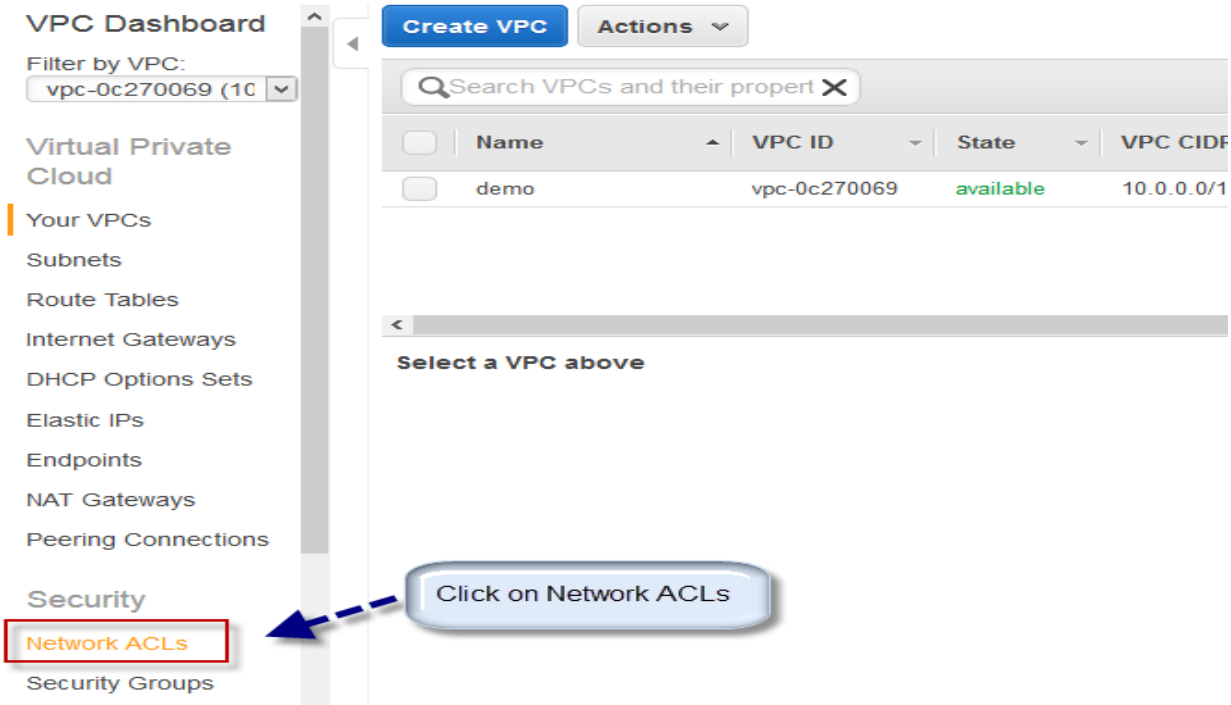
Flow logs: Capture information about the IP traffic going to and from network interfaces in your VPC

Network access control lists (ACLs)

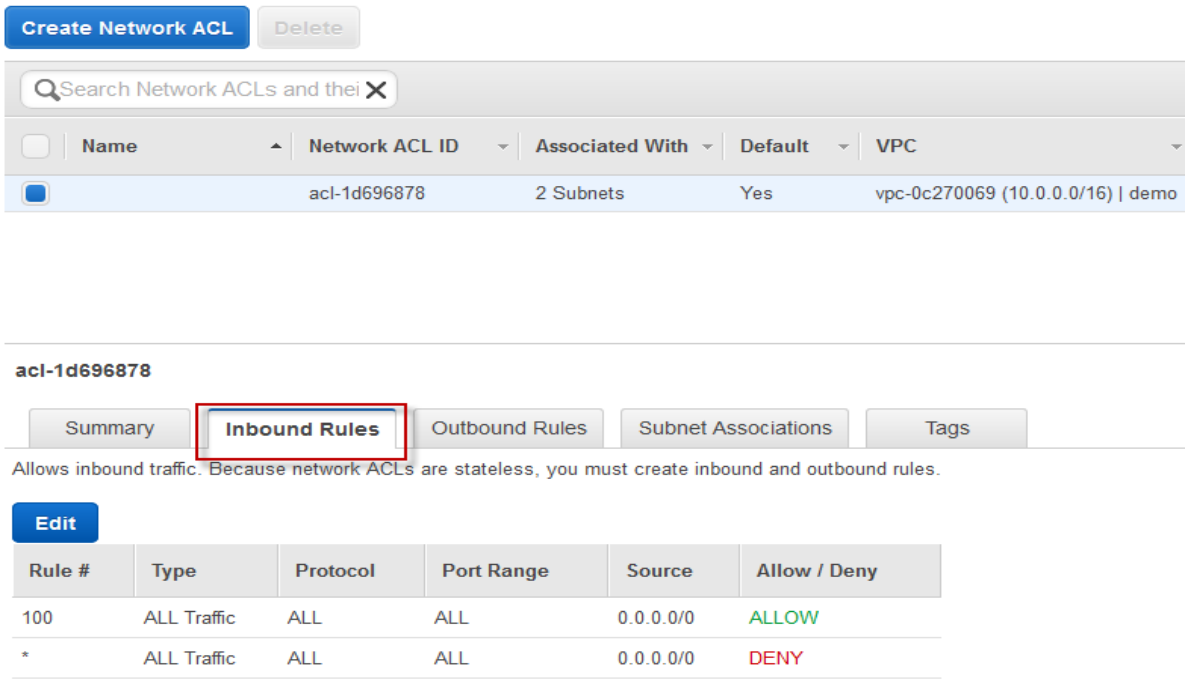
Once you are VPC dashboard, click on Filter by VPC and select your VPC from the drop down list.



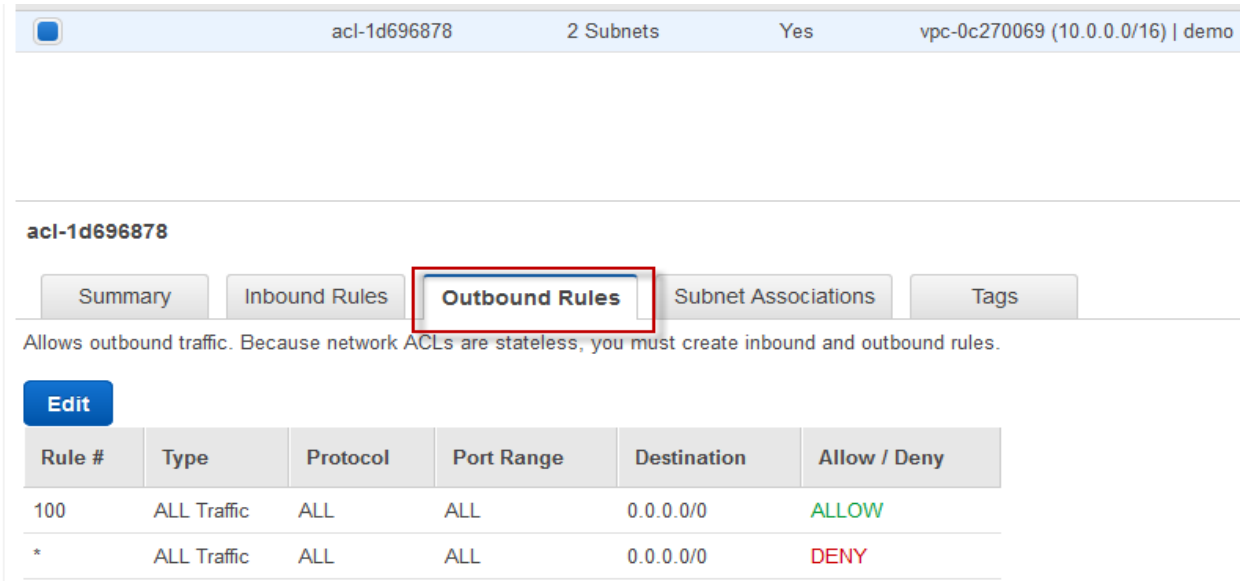
From left pane select Network ACLs under Security.



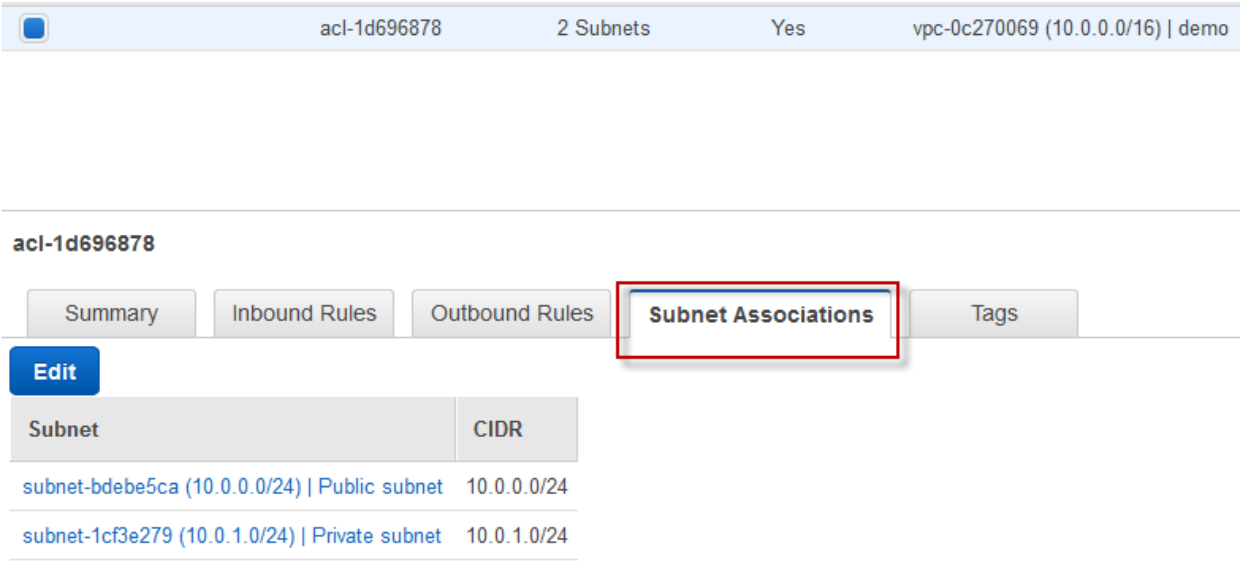
Under Network ACLs page select your NACL and click on Inbound Rules under the page to see the inbound rules.



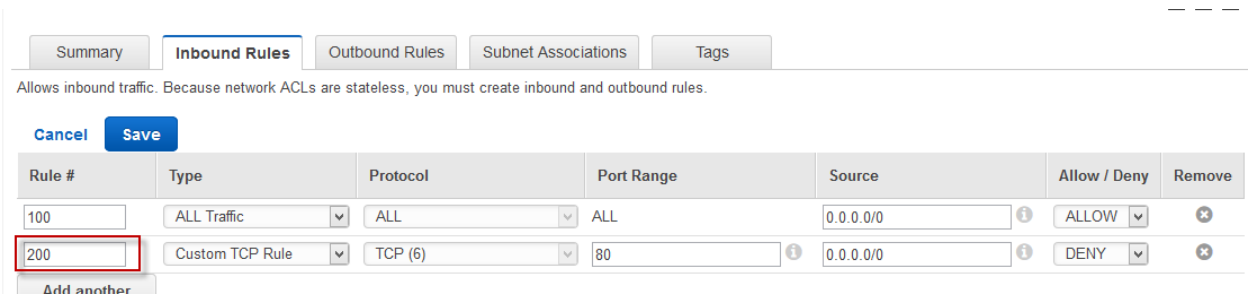
By default, everything is allowed at inbound and as well as outbound.
By click on Outbound rules you can see the default outbound rules.



By clicking on Subnet associations, you can see subnets which are associated with this NACL.



You can click on edit to modify the inbound and outbound rules.
Once clicked on edit, Specify a rule number multiple of 100.
Then specify Type, Protocol, Port range, Source, and Select either ALLOW or DENY.



The same way we can do for outbound rules as well.

FLOW LOGS

IAM Roles for Flow Logs:

The IAM role that's associated with your flow log must have sufficient permissions to publish flow logs to the specified log group in CloudWatch Logs. The IAM policy that's attached to your IAM role must include at least the following permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
```

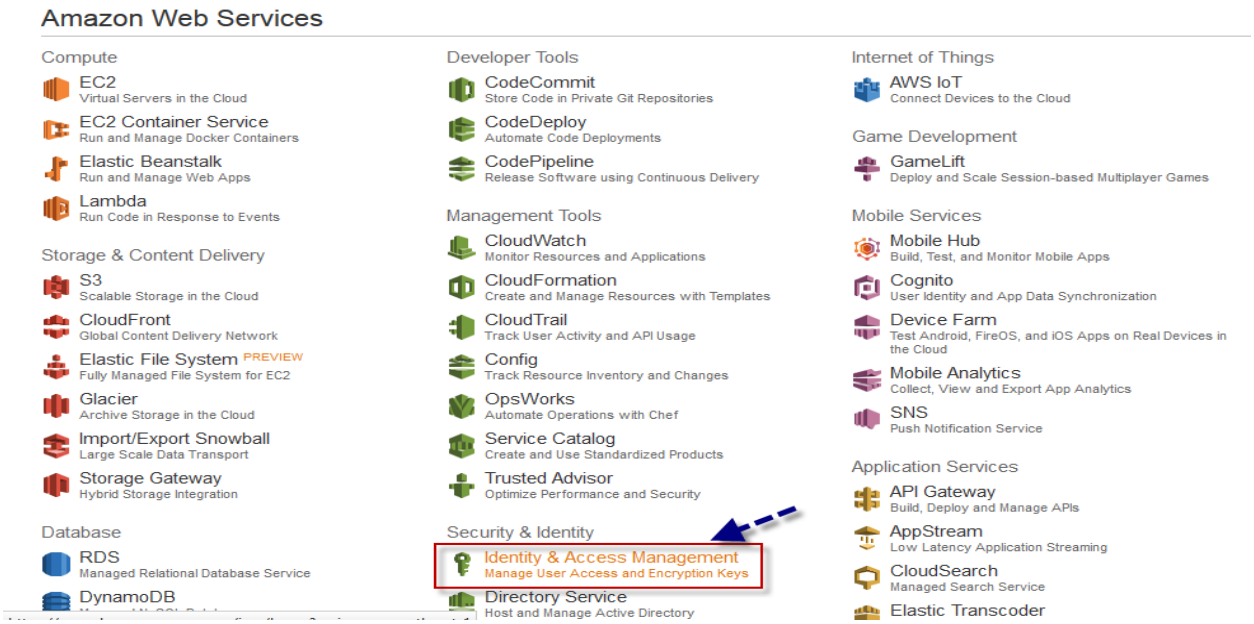
```
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

You must also ensure that your role has a trust relationship that allows the flow logs service to assume the role (in the IAM console, choose your role, and then choose Edit Trust Relationship to view the trust relationship):

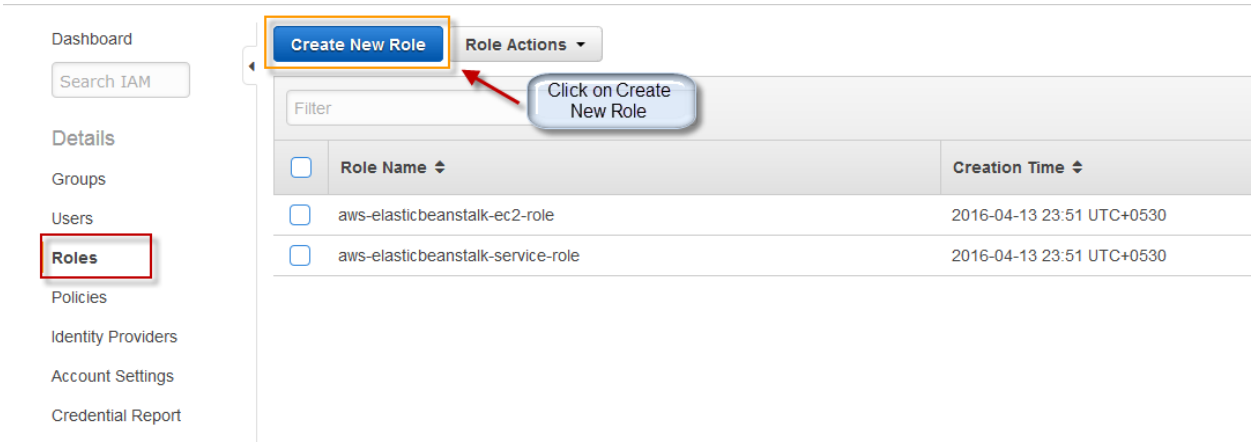
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Alternatively, you can follow the procedures below to create a new role for use with flow logs.

on the aws console page, select Identity & Access Management under Security & Identity.

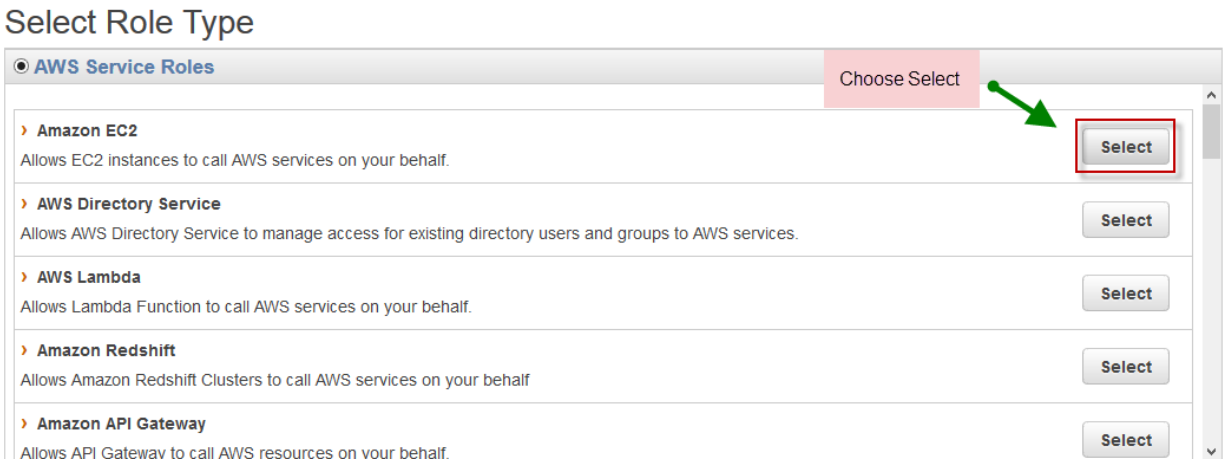


In the left navigation pane, choose Roles, and then choose Create New Role

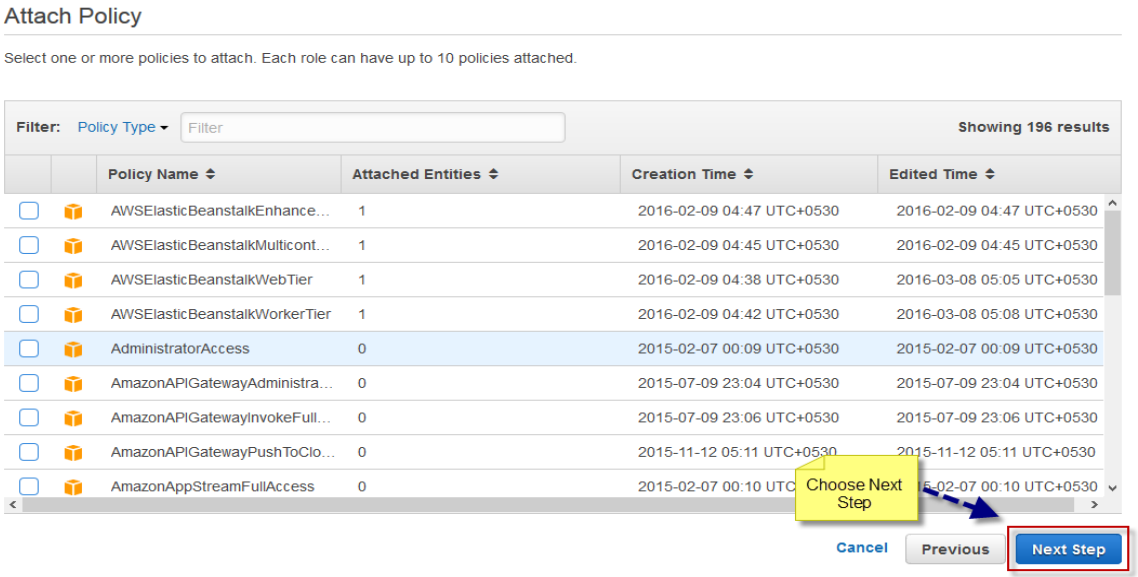


Enter a name for your role and then click Next.

On the Select Role Type page, next to Amazon EC2, choose Select.

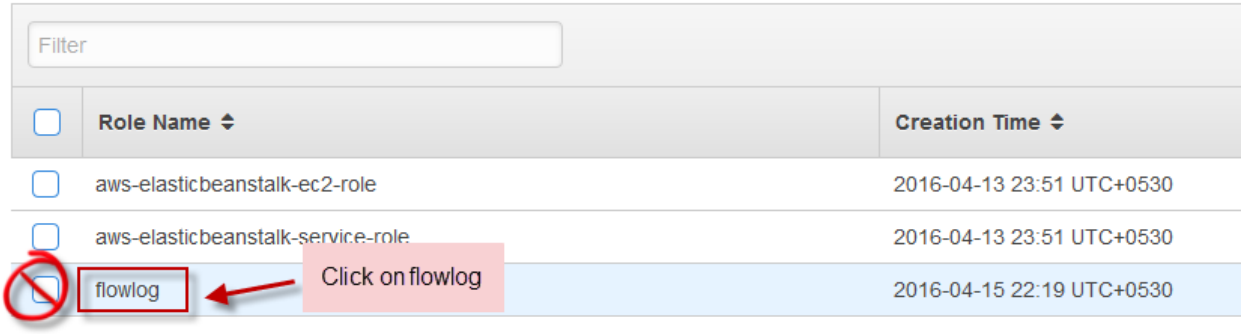


On the Attach Policy page, choose Next Step.

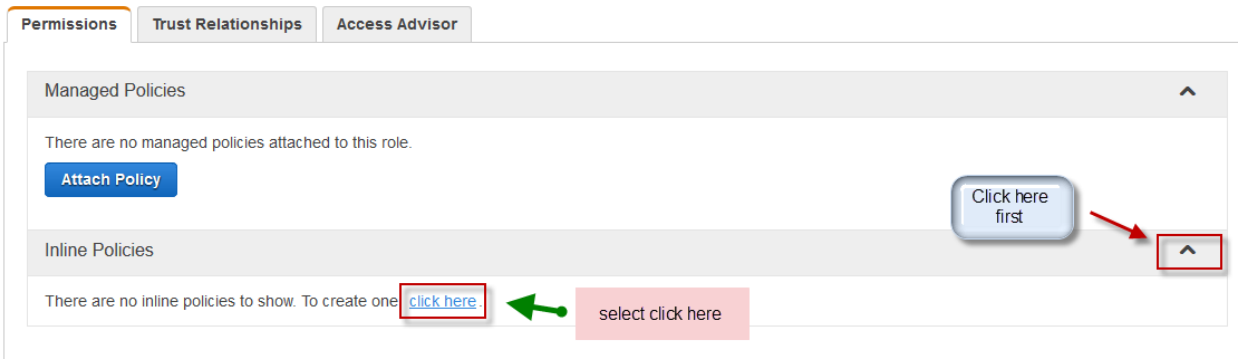


On the Review page, take note of the ARN for your role. You will need this ARN when you create your flow log. When you are ready, choose **Create Role**.

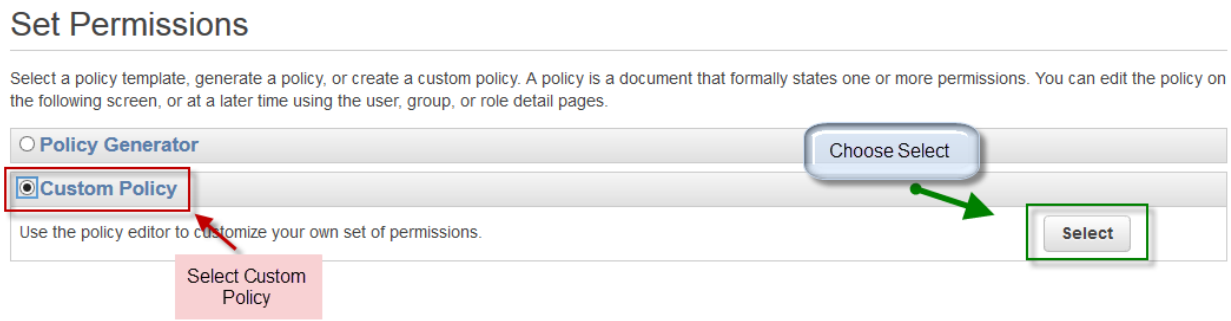
Once done, click on your newly created role name, not on the select role button but on the role name itself.



Under Permissions, expand the Inline Policies section, and then choose click here.

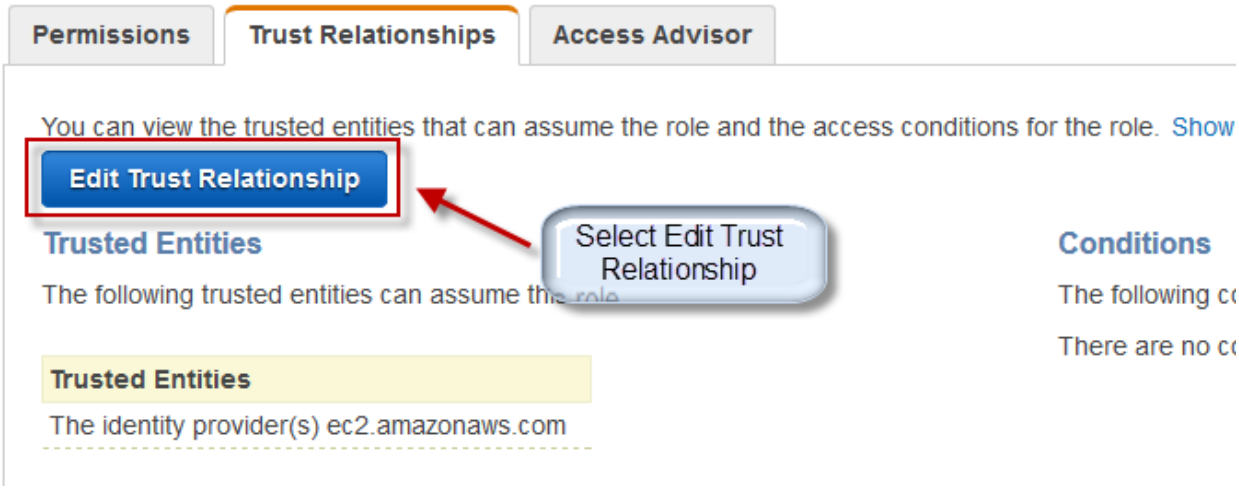


Choose Custom Policy, and then choose Select.

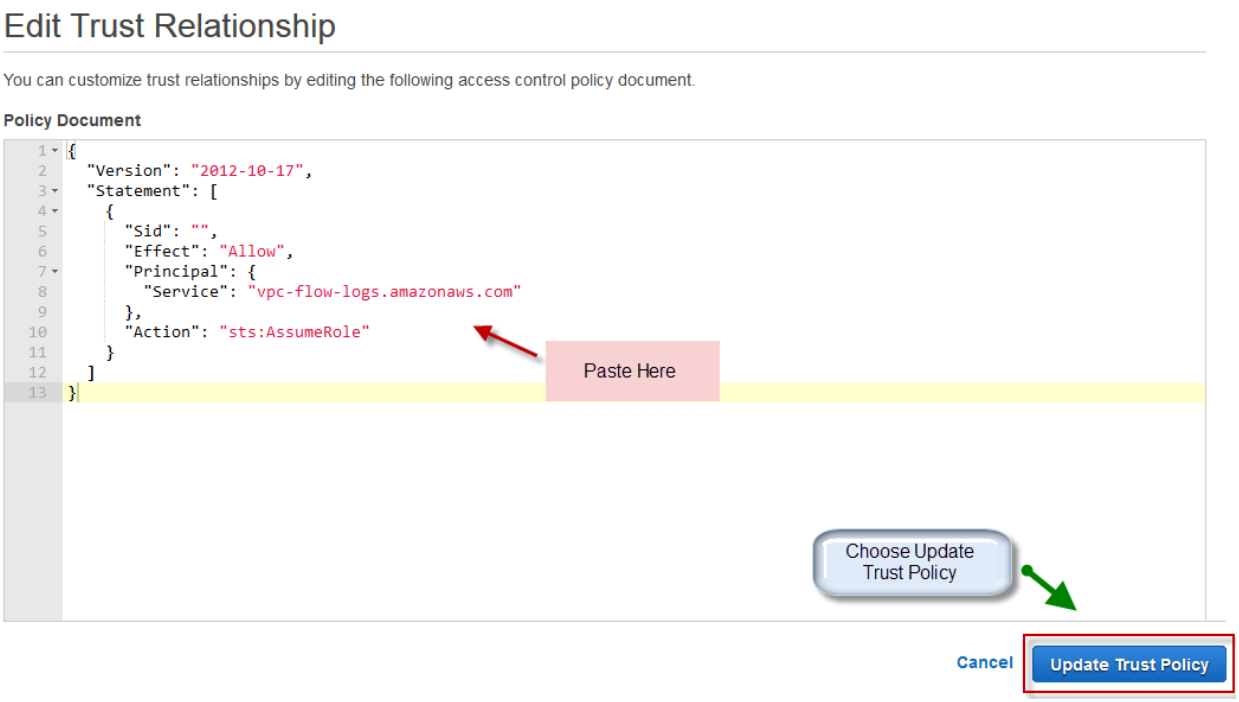


In the section IAM Roles for Flow Logs above, copy the first policy and paste it in thePolicy Document window. Enter a name for your policy in the Policy Name field, and then choose Apply Policy.

choose Edit Trust Relationship under Trust Relationships.

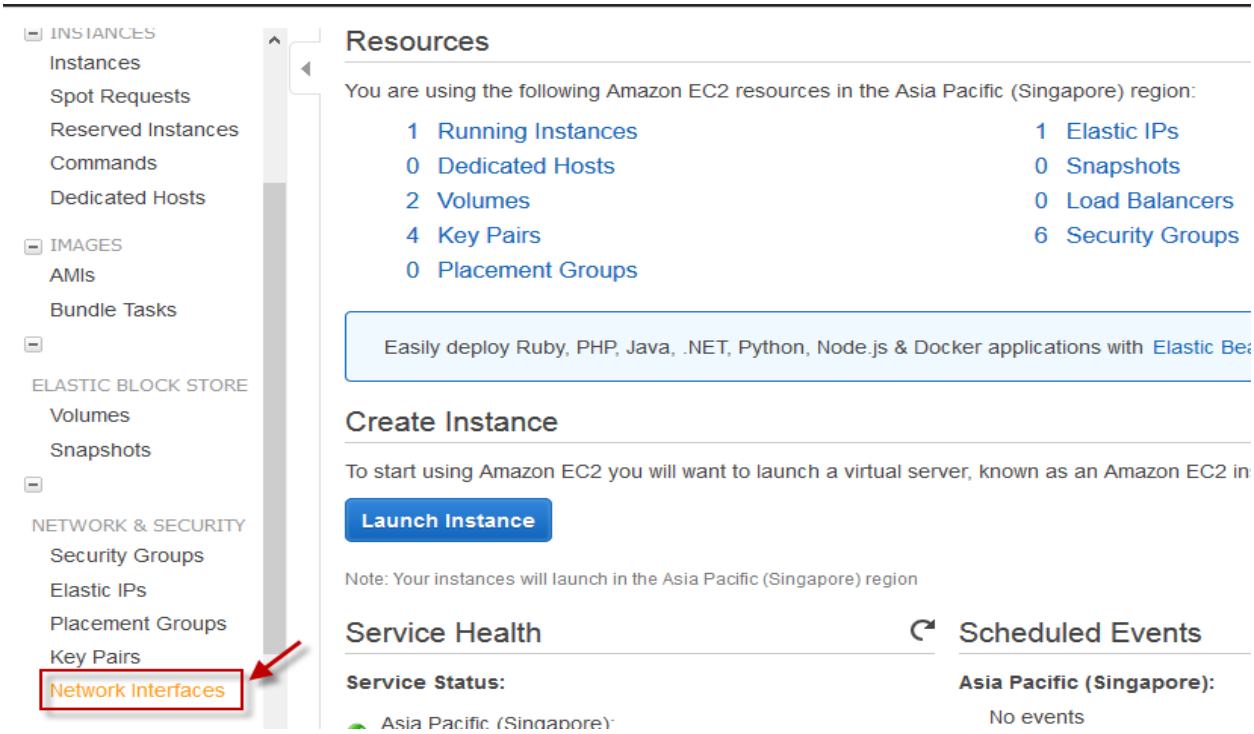


In the section IAM Roles for Flow Logs above, copy the second policy (the trust relationship). Delete the existing policy, and paste in the new one. When you are done, choose Update Trust
Policy.

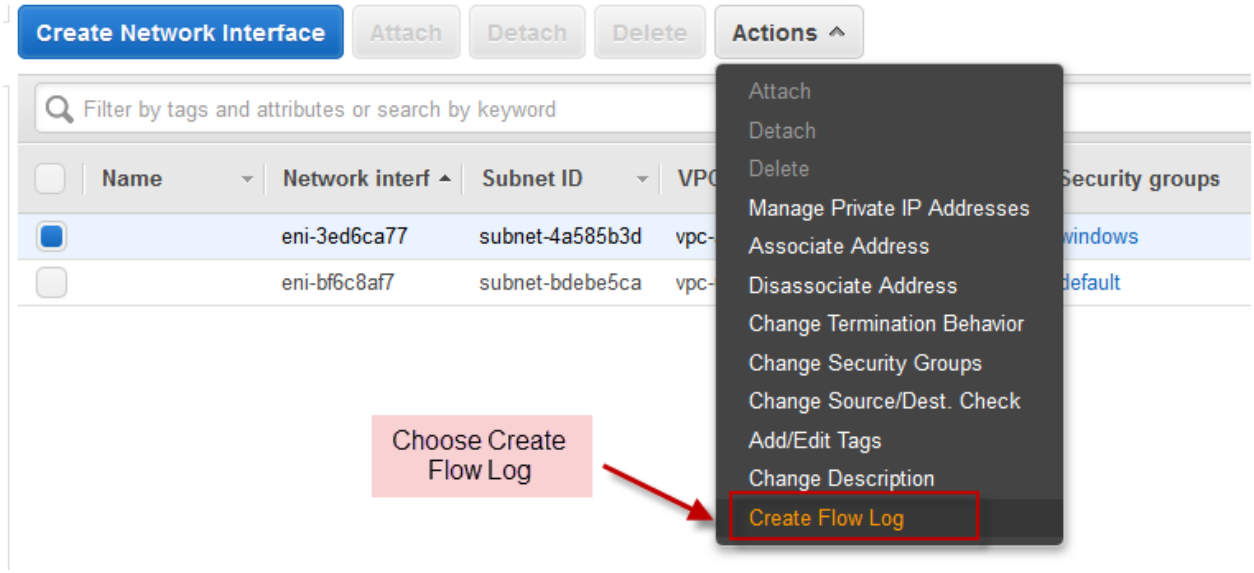


CREATE FLOW LOG FOR EC2 INSTANCE

Once you logged in, choose Network Interfaces under NETWORK & SECURITY from EC2 left navigation pane.



On the network interfaces page, select your instance interface, then under Actions tab select Create Flow Log.

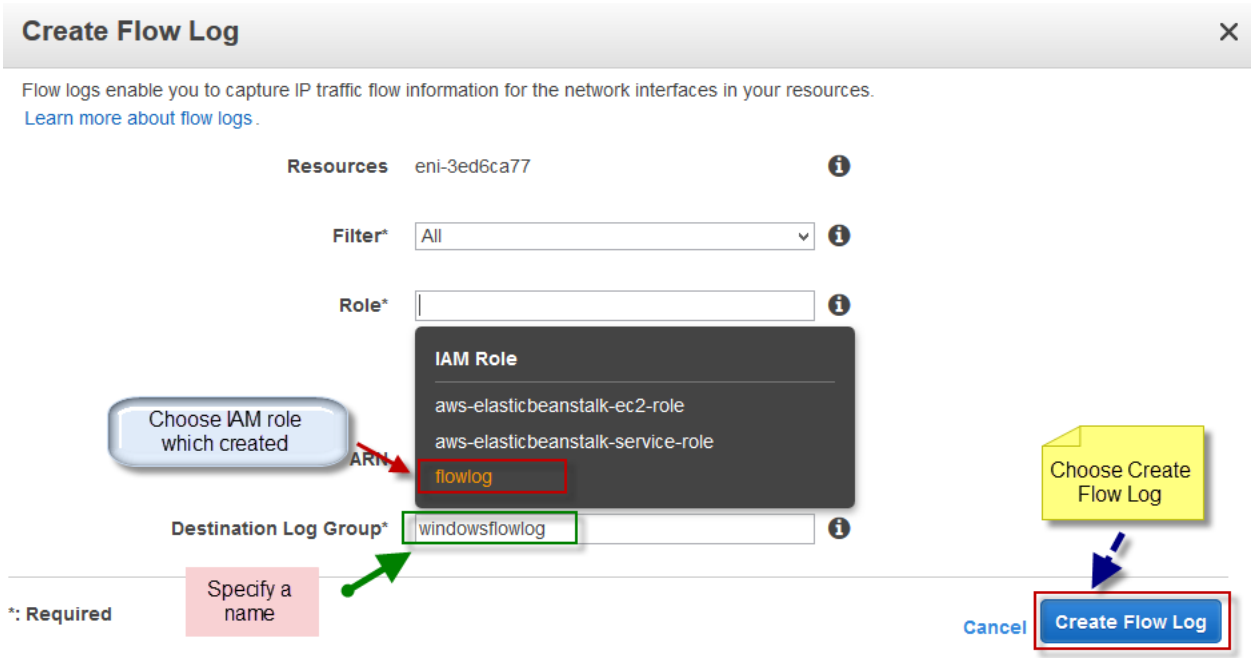


In the dialog box, complete following information. When you are done, choose Create Flow Log.

- **Filter:** Select whether the flow log should capture rejected traffic, accepted traffic, or all traffic.

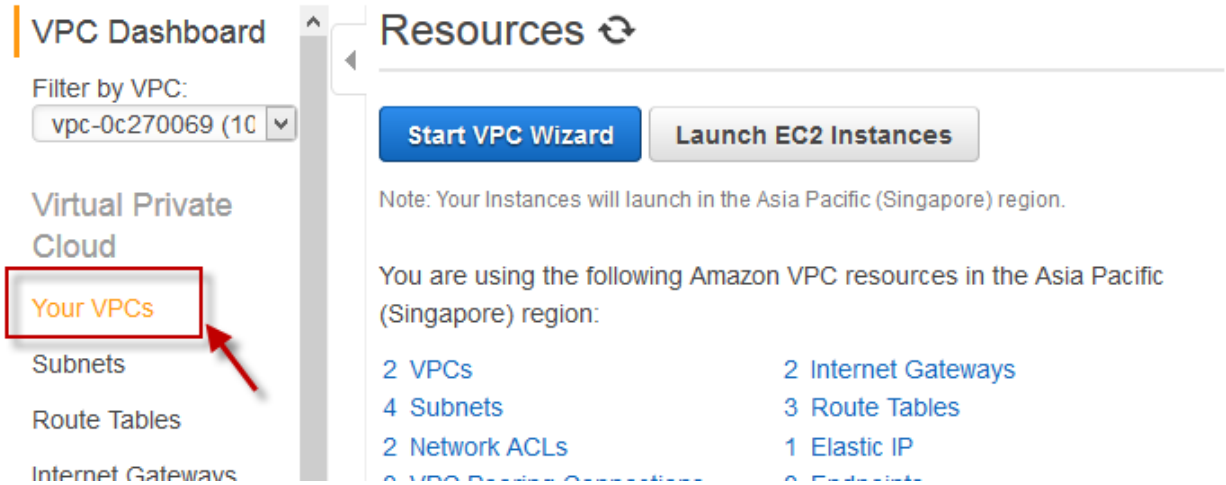
- **Role:** Specify the name of an IAM role that has permission to publish logs to CloudWatch Logs.

- **Destination Log Group:** Enter the name of a log group in CloudWatch Logs to which the flow logs will be published. You can use an existing log group, or you can enter a name for a new log group, which we'll create for you.

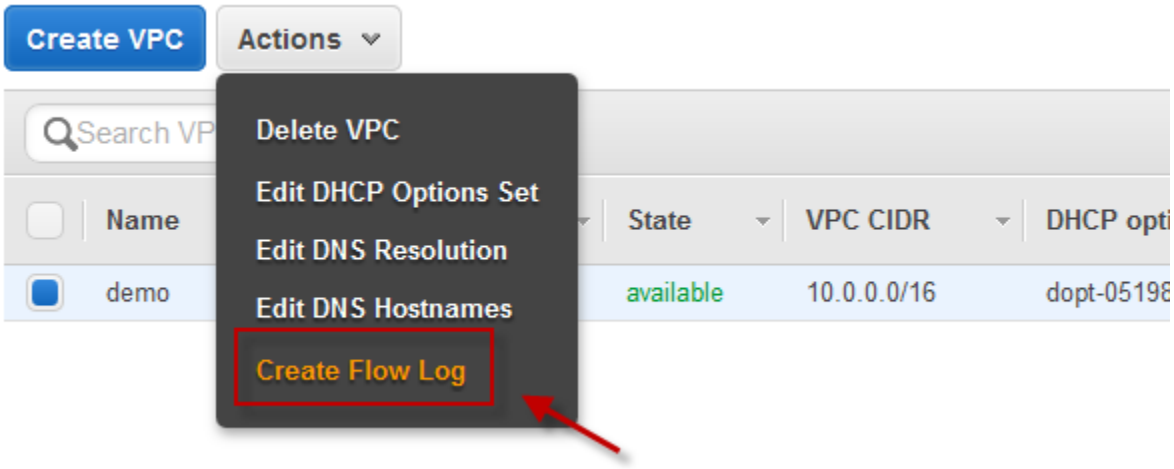


CREATE FLOW LOG FOR A VPC OR A SUBNET

Once you are on VPC page, choose your VPCs or choose subnets.

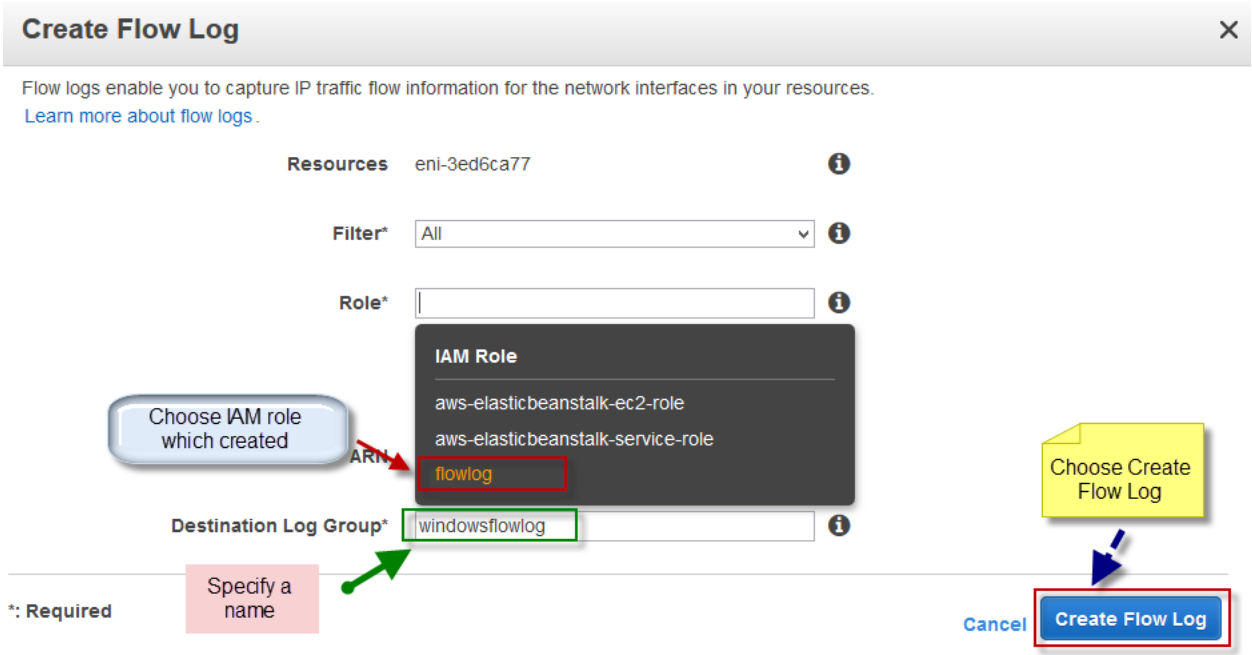


Select your VPC or subnet and click on Actions then select Create Flow Log



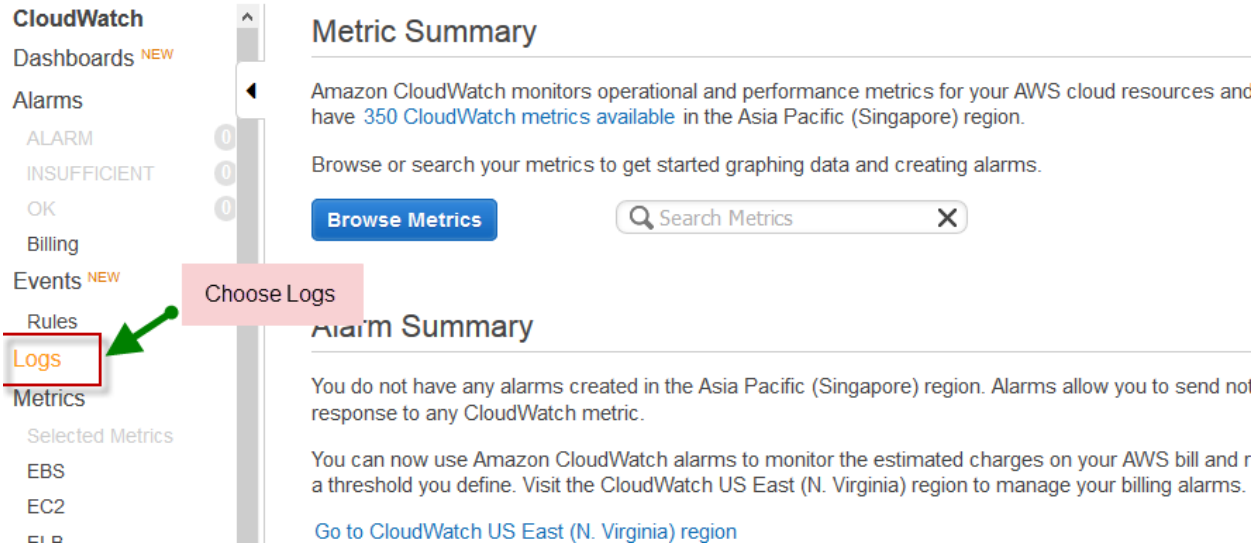
In the dialog box, complete following information. When you are done, choose **Create Flow Log**:

- **Filter**: Select whether the flow log should capture rejected traffic, accepted traffic, or all traffic.
- **Role**: Specify the name of an IAM role that has permission to publish logs to CloudWatch Logs.
- **Destination Log Group**: Enter the name of a log group in CloudWatch Logs to which the flow logs will be published. You can use an existing log group, or you can enter a name for a new log group, which we'll create for you.

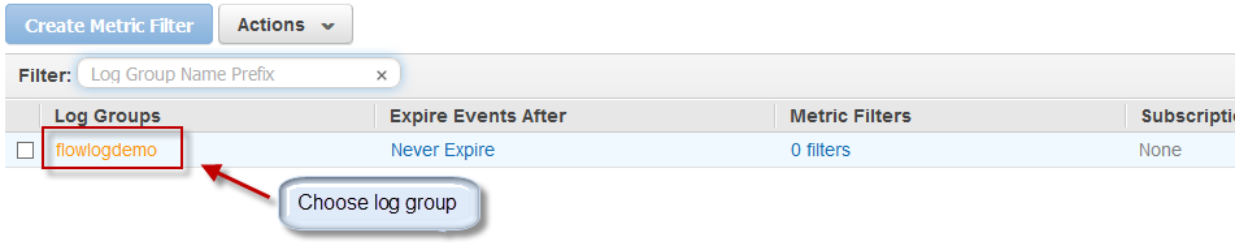


VIEWING FLOW LOGS

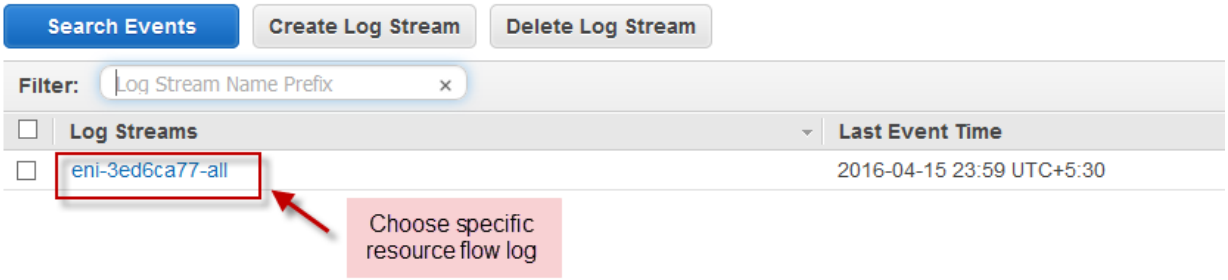
Go to Cloud Watch page from AWS console home.
Once you are in cloudwatch home page, select Logs from the left navigation pane.



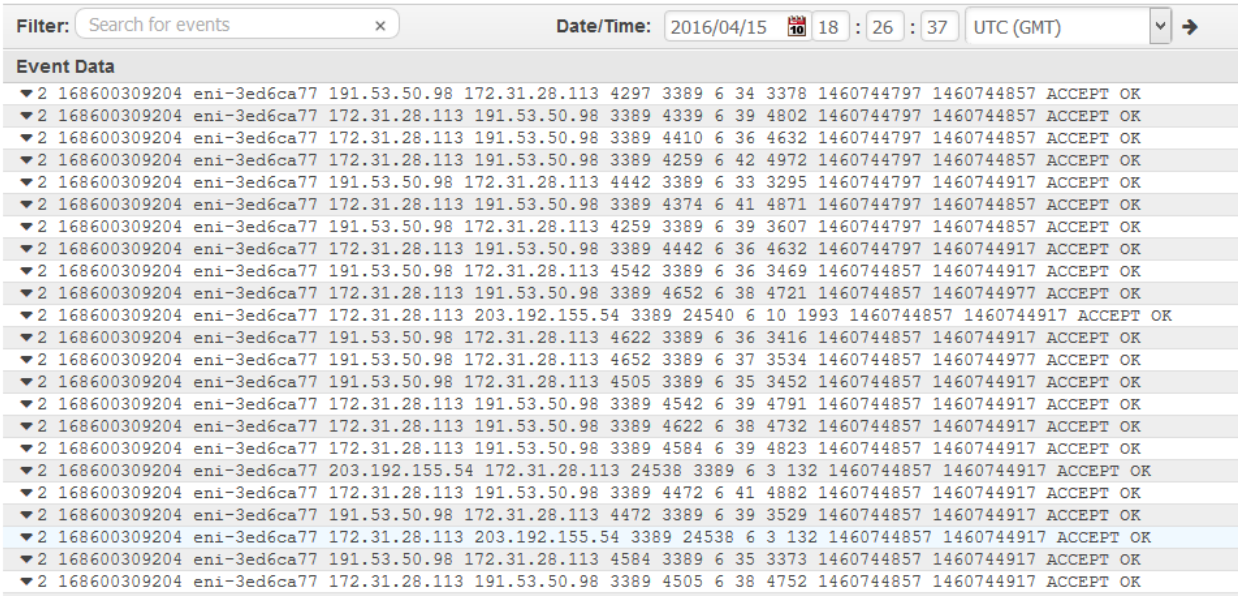
Choose the Log Group which we created for flow log.



Choose specific resource which you want to see the flow log for.

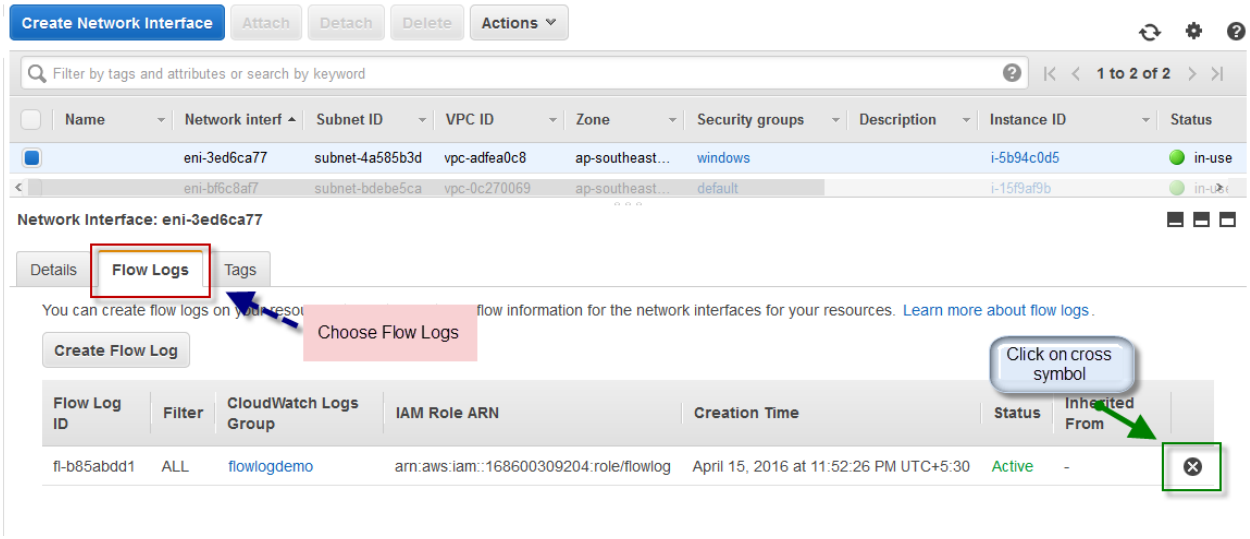


Resource flow log will be displayed like below.



DELETE FLOW LOG

In the navigation pane, choose **Network Interfaces**, and then select the network interface.
Choose the **Flow Logs** tab, and then choose the delete button (a cross) for the flow log to delete.



In the confirmation dialog box, choose **Yes, Delete**.