

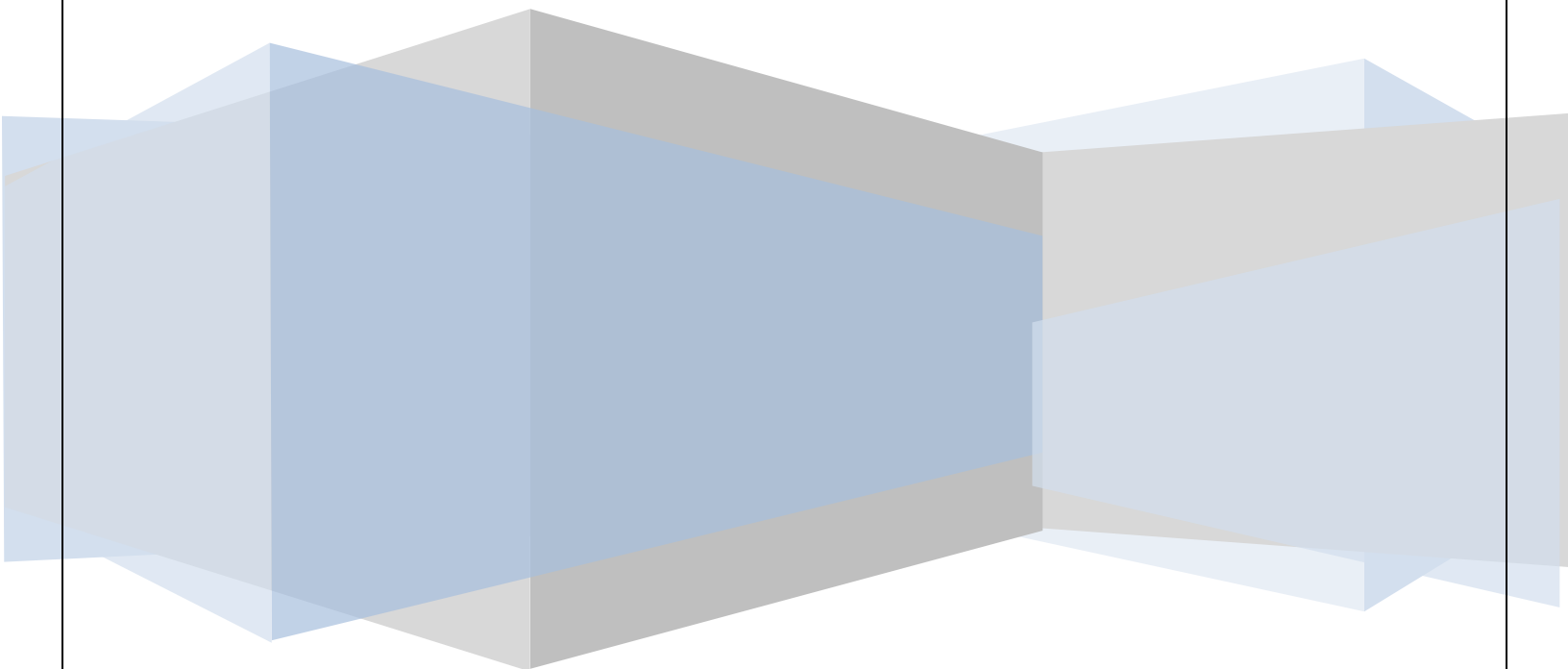


IT TOOK YOU YEARS OF EXPERIENCE
TO REACH WHERE YOU ARE TODAY.
ANOTHER **45 HOURS OF TRAINING**
WITH TACT WILL TAKE YOU HIGHER.

TACT is an online technology academy for competency training to train the IT professionals and uplift their career to discover more opportunities in the space of emerging technologies.

AWS Cloud Training

AWS VIRTUAL PRIVATE CLOUD (VPC)



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.

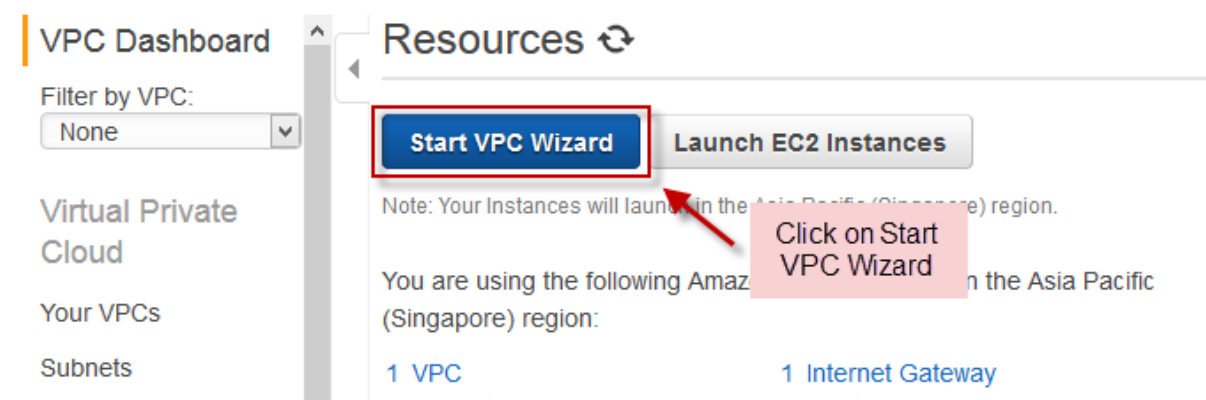
VPC CONFIGURATION

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.

Step 1: Select a VPC Configuration

The screenshot shows the AWS VPC console's 'Create VPC' page. On the left, a list of VPC configurations is shown. The option 'VPC with Public and Private Subnets' is highlighted with a red box and a blue arrow. A pink box with the text 'Select this option' points to this configuration. Below the list, a blue 'Select' button is highlighted with a red box and a green arrow. A blue button labeled 'Click on Select' has a green arrow pointing to the 'Select' button. To the right, a diagram illustrates the VPC architecture: an 'Amazon Virtual Private Cloud' containing a 'Public Subnet' and a 'Private Subnet'. The 'Public Subnet' is connected to the 'Internet, S3, DynamoDB, SNS, SQS, etc.' cloud. The 'Private Subnet' is connected to the 'Public Subnet' via a 'NAT' device. Text explains that in addition to 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). It also states that public subnet instances use Elastic IP addresses to access the Internet, while private subnet instances use NAT. (Hourly charges for NAT devices apply.)

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.

Step 2: VPC with Public and Private Subnets

The screenshot shows the configuration page for creating a VPC with public and private subnets. The form fields are as follows:

- IP CIDR block:** 10.0.0.0/16 (65531 IP addresses available)
- VPC name:** demo
- Public subnet:** 10.0.0.0/24 (251 IP addresses available)
- Availability Zone:** ap-southeast-1a
- Public subnet name:** Public subnet
- Private subnet:** 10.0.1.0/24 (251 IP addresses available)
- Availability Zone:** ap-southeast-1b
- Private subnet name:** Private subnet

At the bottom, it states: 'You can add more subnets after AWS creates the VPC.'

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

Specify the details of your NAT gateway (NAT gateway rates apply).

Elastic IP Allocation ID:*

Add endpoints for S3 to your subnets

Subnet: None

Enable DNS hostnames:*

Hardware tenancy:*

Click here to select NAT instance

Use a NAT instance instead

Cancel and Exit Back Create VPC

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**.

Specify the details of your NAT instance (Instance rates apply).

Instance type:*

Key pair name:*

Add endpoints for S3 to your subnets

Subnet: None

Enable DNS hostnames:*

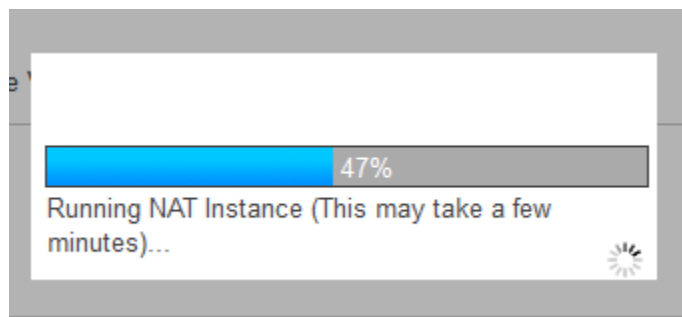
Hardware tenancy:*

Click on Create VPC

Use a NAT gateway instead

Cancel and Exit Back 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.

VPC Successfully Created

Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see [Launching an Instance into Your Subnet](#).

OK

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

You can be able to see the created VPC.

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

- Your VPCs**
- Subnets
- Route Tables
- Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- NAT Gateways
- Peering Connections
- Security

Create VPC **Actions**

Search VPCs and their properties

	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table
<input checked="" type="checkbox"/>	demo	vpc-0c270069	available	10.0.0.0/16	dopt-05198260	rtb-819799e4
<input type="checkbox"/>		vpc-adfea0c8	available	172.31.0.0/16	dopt-05198260	rtb-0ecac6b6

vpc-0c270069 (10.0.0.0/16) | demo

Summary **Flow Logs** **Tags**

VPC ID:	vpc-0c270069 demo	Network ACL:	acl-1d696878
State:	available	Tenancy:	Default
VPC CIDR:	10.0.0.0/16	DNS resolution:	yes
DHCP options set:	dopt-05198260	DNS hostnames:	yes
Route table:	rtb-819799e4	ClassicLink DNS Support:	no

Security in Your VPC

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

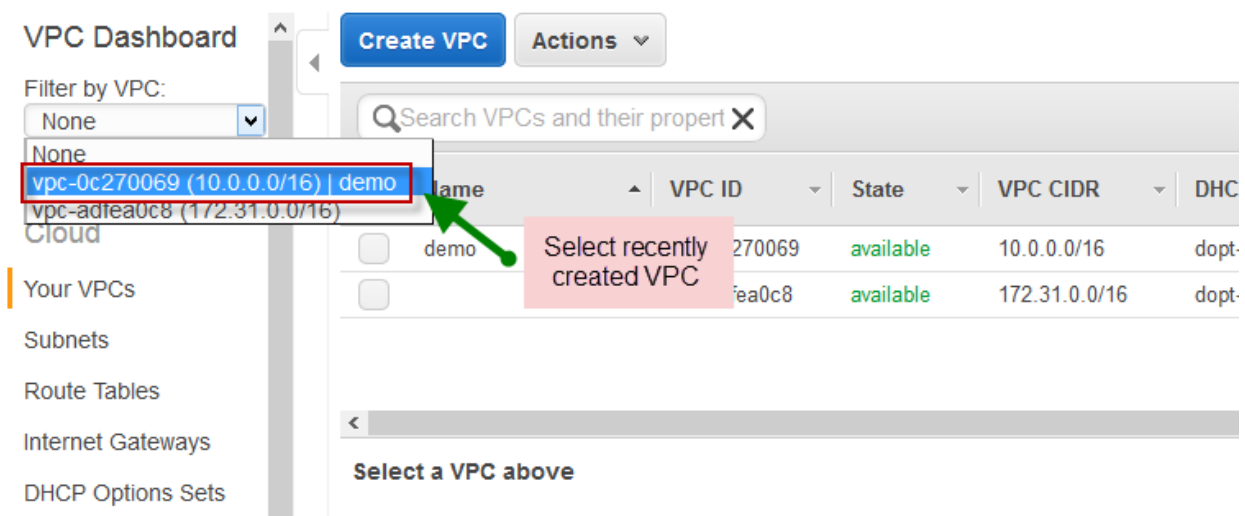
Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level

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.



VPC Dashboard

Create VPC Actions

Filter by VPC:

None

None

vpc-0c270069 (10.0.0.0/16) | demo

vpc-ad7ea0c8 (172.31.0.0/16)

Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Search VPCs and their properties

	VPC ID	State	VPC CIDR	DHC
<input type="checkbox"/> demo	270069	available	10.0.0.0/16	dopt-
<input type="checkbox"/>	7ea0c8	available	172.31.0.0/16	dopt-

Select a VPC above

Select recently created VPC

From left pane select Network ACLs under Security.

VPC Dashboard

Filter by VPC: vpc-0c270069 (10)

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- NAT Gateways
- Peering Connections
- Security**
 - Network ACLs**
 - Security Groups

Create VPC **Actions**

Search VPCs and their properties

<input type="checkbox"/>	Name	VPC ID	State	VPC CIDR
<input type="checkbox"/>	demo	vpc-0c270069	available	10.0.0.0/16

Select a VPC above

Click on Network ACLs

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

Create Network ACL **Delete**

Search Network ACLs and their properties

<input type="checkbox"/>	Name	Network ACL ID	Associated With	Default	VPC
<input checked="" type="checkbox"/>		acl-1d696878	2 Subnets	Yes	vpc-0c270069 (10.0.0.0/16) demo

acl-1d696878

Summary **Inbound Rules** **Outbound Rules** **Subnet Associations** **Tags**

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

☐
acl-1d696878
2 Subnets
Yes
vpc-0c270069 (10.0.0.0/16) | demo

acl-1d696878

Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

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

☐
acl-1d696878
2 Subnets
Yes
vpc-0c270069 (10.0.0.0/16) | demo

acl-1d696878

Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags

Edit

Subnet	CIDR
subnet-bdebe5ca (10.0.0.0/24) Public subnet	10.0.0.0/24
subnet-1cf3e279 (10.0.1.0/24) Private subnet	10.0.1.0/24

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.

— — —

Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Cancel
Save

Rule #	Type	Protocol	Port Range	Source	Allow / Deny	Remove
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW	✕
200	Custom TCP Rule	TCP (6)	80	0.0.0.0/0	DENY	✕

Add another

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:

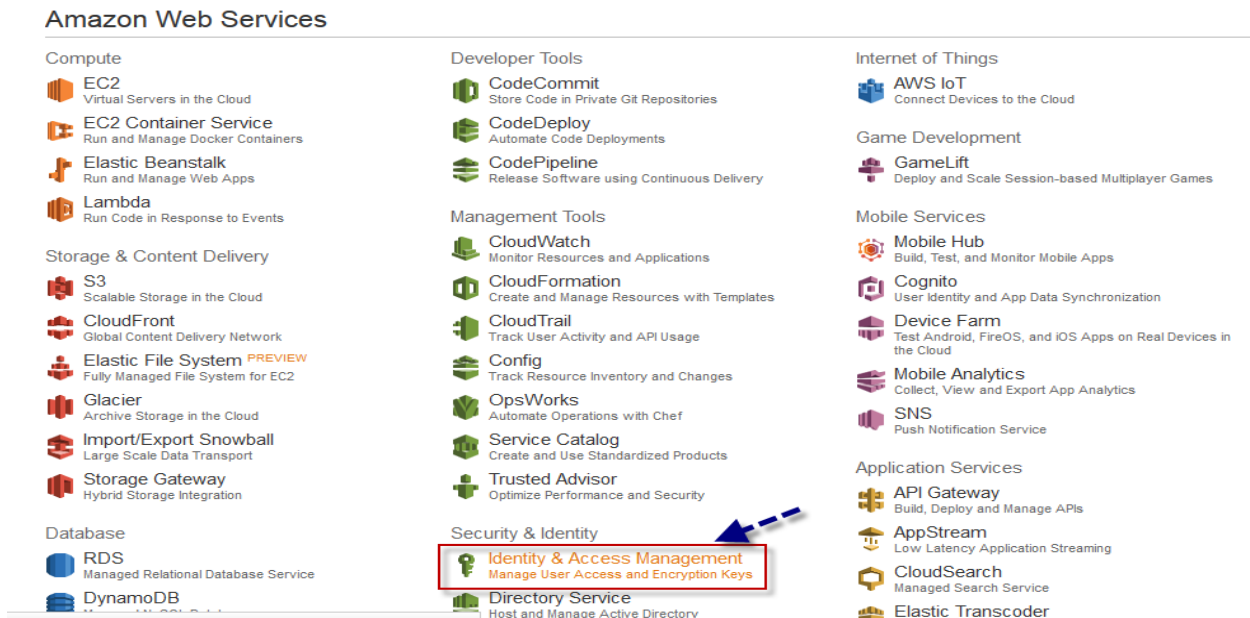
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

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):

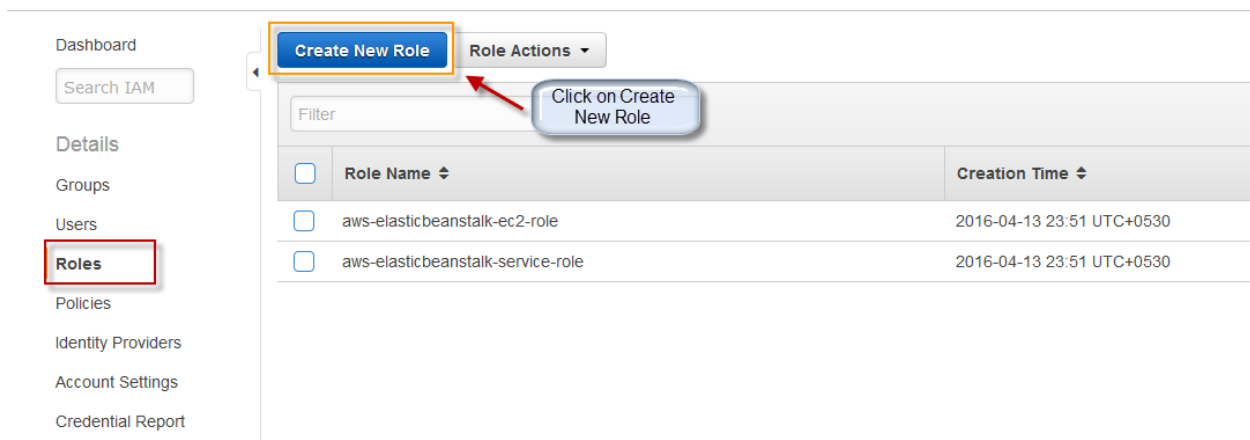
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

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.

Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name
Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-', '_' characters

Specify a name

Cancel **Next Step**

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

Select Role Type

AWS Service Roles Choose Select

Amazon EC2 Allows EC2 instances to call AWS services on your behalf.	Select
AWS Directory Service Allows AWS Directory Service to manage access for existing directory users and groups to AWS services.	Select
AWS Lambda Allows Lambda Function to call AWS services on your behalf.	Select
Amazon Redshift Allows Amazon Redshift Clusters to call AWS services on your behalf	Select
Amazon API Gateway Allows API Gateway to call AWS resources on your behalf.	Select

On the Attach Policy page, choose Next Step.

Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

Filter: Policy Type Showing 196 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AWSElasticBeanstalkEnhance...	1	2016-02-09 04:47 UTC+0530	2016-02-09 04:47 UTC+0530
<input type="checkbox"/>	AWSElasticBeanstalkMulticont...	1	2016-02-09 04:45 UTC+0530	2016-02-09 04:45 UTC+0530
<input type="checkbox"/>	AWSElasticBeanstalkWebTier	1	2016-02-09 04:38 UTC+0530	2016-03-08 05:05 UTC+0530
<input type="checkbox"/>	AWSElasticBeanstalkWorkerTier	1	2016-02-09 04:42 UTC+0530	2016-03-08 05:08 UTC+0530
<input type="checkbox"/>	AdministratorAccess	0	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayAdministra...	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayInvokeFull...	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayPushToClo...	0	2015-11-12 05:11 UTC+0530	2015-11-12 05:11 UTC+0530
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530

Choose Next Step

Cancel Previous **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**.

Review

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

Role Name flowlog [Edit Role Name](#)

Role ARN arn:aws:iam::168600309204:role/flowlog

Trusted Entities The identity provider(s) ec2.amazonaws.com

Policies [Change Policies](#)



Cancel Previous **Create Role**

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

Filter		
<input type="checkbox"/>	Role Name ↕	Creation Time ↕
<input type="checkbox"/>	aws-elasticbeanstalk-ec2-role	2016-04-13 23:51 UTC+0530
<input type="checkbox"/>	aws-elasticbeanstalk-service-role	2016-04-13 23:51 UTC+0530
<input checked="" type="checkbox"/>	flowlog	2016-04-15 22:19 UTC+0530

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

Permissions
Trust Relationships
Access Advisor

Managed Policies

There are no managed policies attached to this role.

Attach Policy

Inline Policies

There are no inline policies to show. To create one [click here](#)

Choose Custom Policy, and then choose Select.

Set Permissions

Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.

☐ Policy Generator
☒ Custom Policy

Choose Select


Select

Use the policy editor to customize your own set of permissions.

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

Review Policy

Customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies](#) in the *Using IAM* guide. To test the effects of this policy before applying your changes, use the [IAM Policy Simulator](#).


Policy Name
flowlog  Specify a name


Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "logs:CreateLogGroup",
7         "logs:CreateLogStream",
8         "logs:PutLogEvents",
9         "logs:DescribeLogGroups",
10        "logs:DescribeLogStreams"
11      ],
12      "Effect": "Allow",
13      "Resource": "*"
14    }
15  ]
16 }

```

 Paste here

 Choose Apply Policy


☒ Use autoformatting for policy editing

Cancel Validate Policy **Apply Policy**

choose Edit Trust Relationship under Trust Relationships.

Permissions **Trust Relationships** Access Advisor

You can view the trusted entities that can assume the role and the access conditions for the role. [Show](#)

Edit Trust Relationship  Select Edit Trust Relationship

Trusted Entities

The following trusted entities can assume this role.

Trusted Entities

The identity provider(s) ec2.amazonaws.com

Conditions

The following conditions are associated with this role.

There are no conditions associated with this role.

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.

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "",
6       "Effect": "Allow",
7       "Principal": {
8         "Service": "vpc-flow-logs.amazonaws.com"
9       },
10      "Action": "sts:AssumeRole"
11    }
12  ]
13 }
```

Paste Here

Choose Update Trust Policy

Cancel
Update Trust Policy

CREATE FLOW LOG FOR EC2 INSTANCE

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

The screenshot shows the AWS Management Console interface. On the left, the 'NETWORK & SECURITY' section is expanded, and 'Network Interfaces' is highlighted with a red box and a red arrow. The main content area shows the 'Resources' section for the Asia Pacific (Singapore) region, listing various EC2 resources like Running Instances, Elastic IPs, etc. Below this, there's a 'Create Instance' section and a 'Service Health' section.

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

The screenshot shows the 'Network Interfaces' page in the AWS console. A table lists network interfaces with columns for Name, Network interface, Subnet ID, and VPC. The first interface, 'eni-3ed6ca77', is selected. The 'Actions' dropdown menu is open, showing various actions like 'Attach', 'Detach', 'Delete', 'Manage Private IP Addresses', etc. The 'Create Flow Log' option is highlighted with a red box, and a red arrow points to it from a pink box labeled 'Choose 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

×

Flow logs enable you to capture IP traffic flow information for the network interfaces in your resources.
[Learn more about flow logs.](#)

Resources

eni-3ed6ca77

ⓘ

Filter*

All

⌵

ⓘ

Role*

ⓘ

Choose IAM role which created

ARN

IAM Role

aws-elasticbeanstalk-ec2-role

aws-elasticbeanstalk-service-role

flowlog

Destination Log Group*

windowsflowlog

ⓘ

Specify a name

⬆

Cancel

Create Flow Log

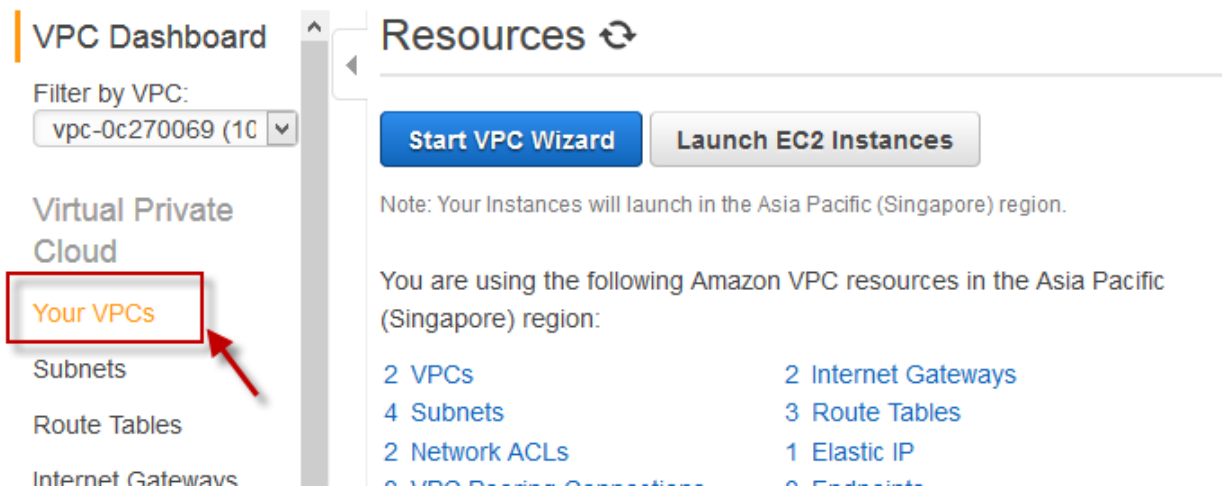
⌵

⬆

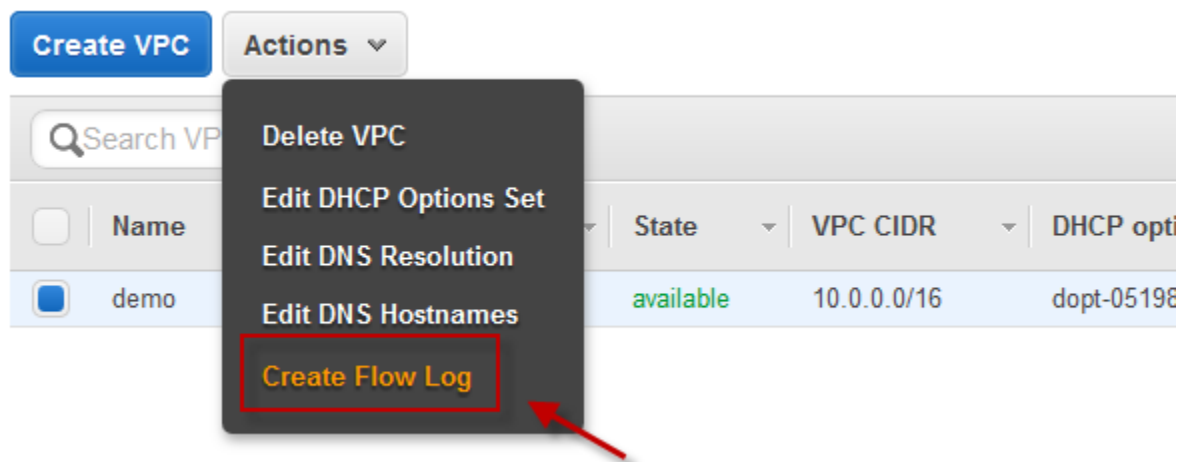
*: Required

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.

Create Flow Log

×

Flow logs enable you to capture IP traffic flow information for the network interfaces in your resources.
[Learn more about flow logs.](#)

Resources eni-3ed6ca77 ⓘ

Filter* All ⓘ

Role* ⓘ

Choose IAM role which created

ARN

IAM Role
aws-elasticbeanstalk-ec2-role
aws-elasticbeanstalk-service-role
flowlog

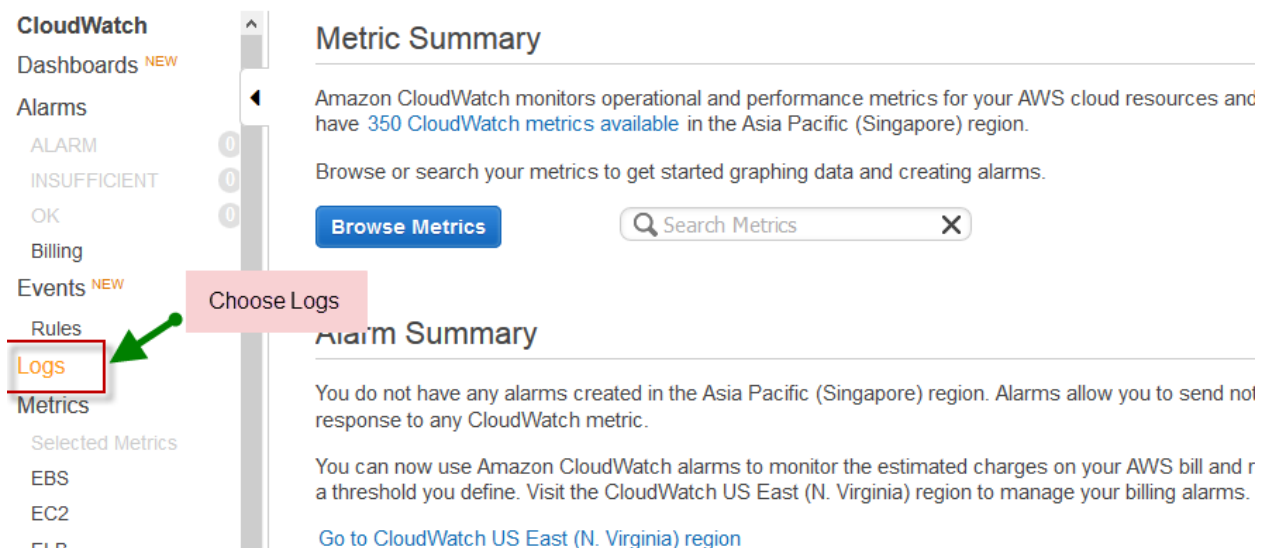
Destination Log Group* windowsflowlog ⓘ

Specify a name

Cancel Create Flow Log

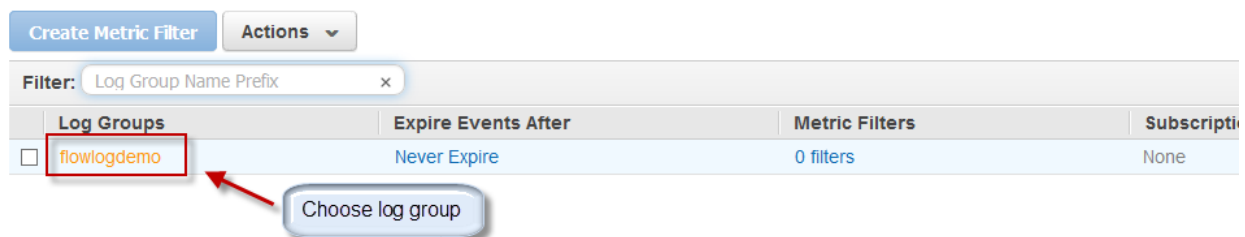
VIEWING FLOW LOGS

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



The screenshot shows the AWS CloudWatch console interface. On the left, the navigation pane is visible with the following items: CloudWatch, Dashboards ^{NEW}, Alarms, Events ^{NEW}, Rules, **Logs** (highlighted with a red box and a green arrow), Metrics, and Selected Metrics. A pink callout box labeled 'Choose Logs' points to the 'Logs' item. The main content area displays the 'Metric Summary' section, which includes a description of Amazon CloudWatch metrics and a 'Browse Metrics' button. Below this, the 'Alarm Summary' section is visible, stating that no alarms are currently created in the Asia Pacific (Singapore) region.

Choose the Log Group which we created for flow log.



The screenshot shows a table of Log Groups in the AWS CloudWatch console. The table has four columns: Log Groups, Expire Events After, Metric Filters, and Subscriptions. The first row contains the log group 'flowlogdemo', which is highlighted with a red box and a red arrow. A blue callout box labeled 'Choose log group' points to the 'flowlogdemo' entry. The table also shows that the log group has 'Never Expire' set for expiration, '0 filters' for metric filters, and 'None' for subscriptions.

Log Groups	Expire Events After	Metric Filters	Subscriptions
flowlogdemo	Never Expire	0 filters	None

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

Search Events

Create Log Stream

Delete Log Stream

Filter: x

<input type="checkbox"/>	Log Streams	Last Event Time
<input type="checkbox"/>	eni-3ed6ca77-all	2016-04-15 23:59 UTC+5:30

Choose specific resource flow log

Resource flow log will be displayed like below.

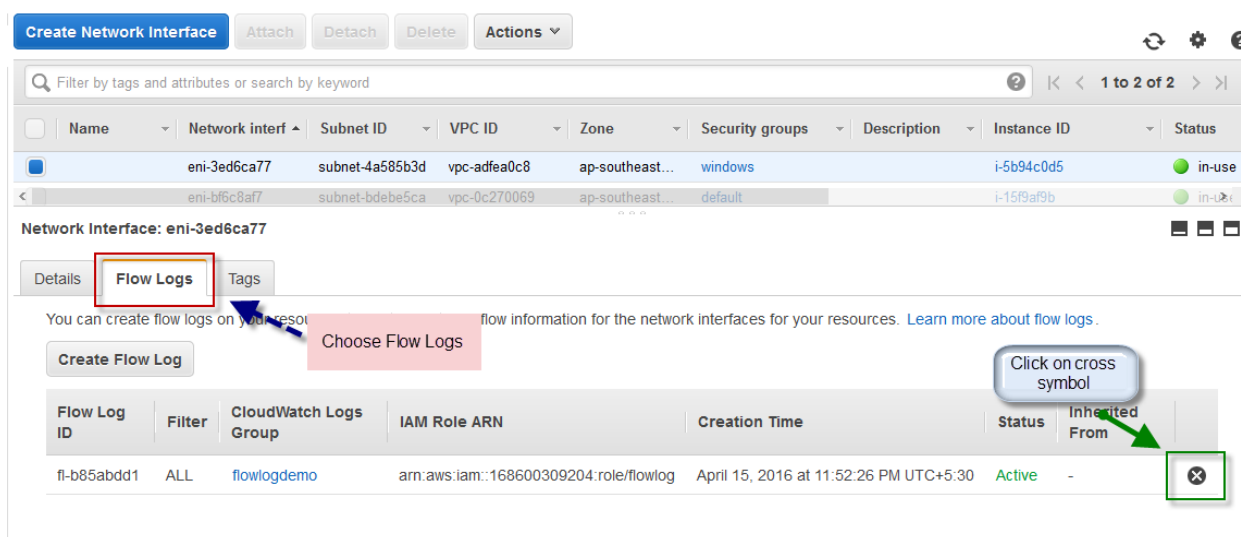
Filter: x
Date/Time: 2016/04/15 18 : 26 : 37 UTC (GMT)

Event Data													
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4297	3389	6	34	3378	1460744797	1460744857	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4339	6	39	4802	1460744797	1460744857	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4410	6	36	4632	1460744797	1460744857	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4259	6	42	4972	1460744797	1460744857	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4442	3389	6	33	3295	1460744797	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4374	6	41	4871	1460744797	1460744857	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4259	3389	6	39	3607	1460744797	1460744857	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4442	6	36	4632	1460744797	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4542	3389	6	36	3469	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4652	6	38	4721	1460744857	1460744977	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	203.192.155.54	3389	24540	6	10	1993	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4622	3389	6	36	3416	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4652	3389	6	37	3534	1460744857	1460744977	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4505	3389	6	35	3452	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4542	6	39	4791	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4622	6	38	4732	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4584	6	39	4823	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	203.192.155.54	172.31.28.113	24538	3389	6	3	132	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4472	6	41	4882	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4472	3389	6	39	3529	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	203.192.155.54	3389	24538	6	3	132	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	191.53.50.98	172.31.28.113	4584	3389	6	35	3373	1460744857	1460744917	ACCEPT	OK
▼ 2	168600309204	eni-3ed6ca77	172.31.28.113	191.53.50.98	3389	4505	6	38	4752	1460744857	1460744917	ACCEPT	OK

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.



Filter by tags and attributes or search by keyword

1 to 2 of 2

Name	Network interf	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID	Status
eni-3ed6ca77	subnet-4a585b3d	vpc-adfea0c8	ap-southeast...	windows	i-5b94c0d5		in-use	
eni-bf6c8af7	subnet-bdebe5ca	vpc-0c270069	ap-southeast...	default	i-15f9af9b		in-use	

Network Interface: eni-3ed6ca77

Details **Flow Logs** Tags

You can create flow logs on your resources to capture flow information for the network interfaces for your resources. [Learn more about flow logs.](#)

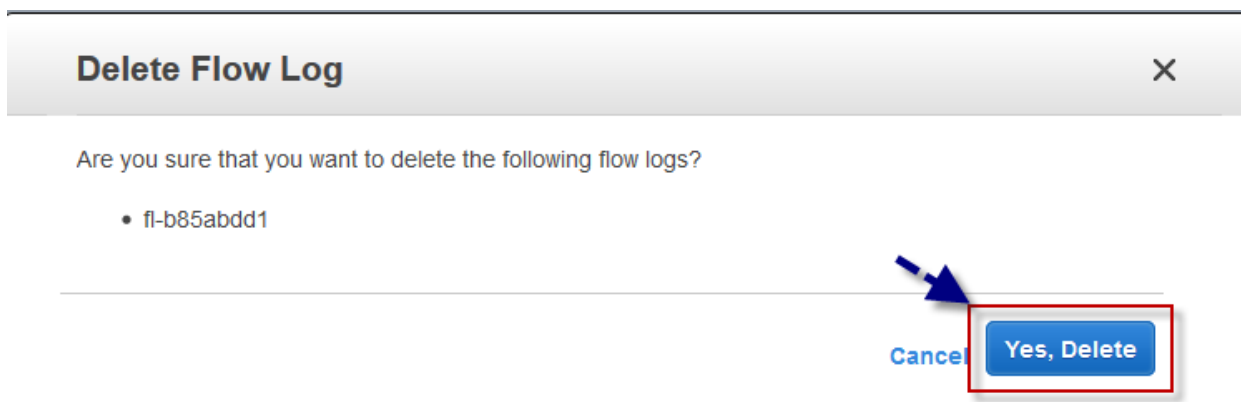
Create Flow Log

Choose Flow Logs

Flow Log ID	Filter	CloudWatch Logs Group	IAM Role ARN	Creation Time	Status	Inherited From	
fl-b85abdd1	ALL	flowlogdemo	arn:aws:iam::168600309204:role/flowlog	April 15, 2016 at 11:52:26 PM UTC+5:30	Active	-	✕

Click on cross symbol

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



Delete Flow Log

Are you sure that you want to delete the following flow logs?

- fl-b85abdd1

Cancel Yes, Delete