

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.

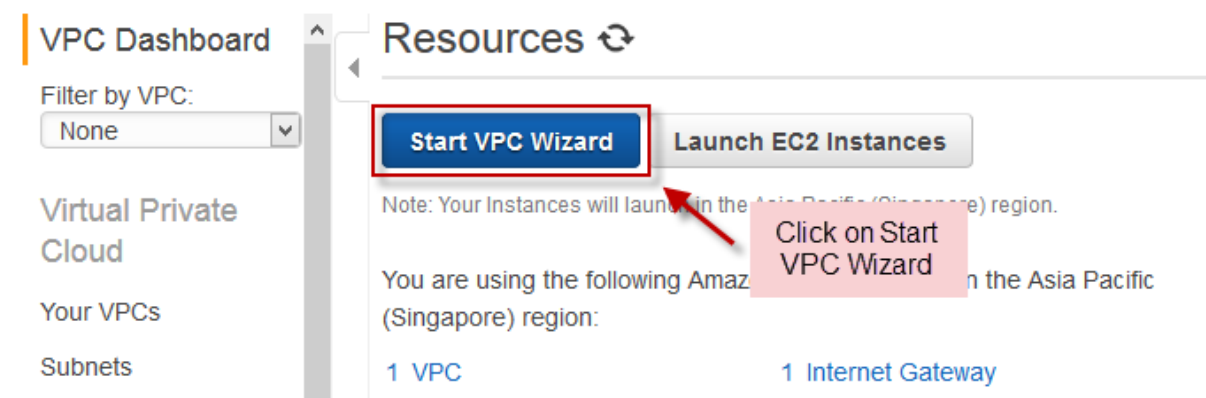
VPC CONFIGURATION

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 'VPC with Public and Private Subnets' option is highlighted with a red box and a blue arrow. A pink box with the text 'Select this option' points to the same option. Below the list, a blue 'Select' button is highlighted with a red box and a green arrow. A 'Click on Select' button with a green arrow points to the 'Select' button. To the right, a diagram illustrates the VPC architecture: a central 'Amazon Virtual Private Cloud' box contains a 'Public Subnet' and a 'Private Subnet'. The 'Public Subnet' is connected to a 'NAT' box, which is in turn connected to the 'Private Subnet'. Above the VPC box, a cloud icon represents the 'Internet, S3, DynamoDB, SNS, SQS, etc.'.

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

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).

Creates:

Select this option with two /24 subnets. Public subnet instances use Elastic IP addresses to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

Click on Select

Select

Internet, S3, DynamoDB, SNS, SQS, etc.

Amazon Virtual Private Cloud

Public Subnet

Private Subnet

NAT

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 'Create VPC' page with the 'VPC with Public and Private Subnets' configuration selected. 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

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:* ☒ Yes ☐ No

Hardware tenancy:* Default

[Use a NAT instance instead](#)

Click here to select NAT instance

[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:* t2.micro

Key pair name: linux

Add endpoints for S3 to your subnets

Subnet: None

Enable DNS hostnames:* ☒ Yes ☐ No

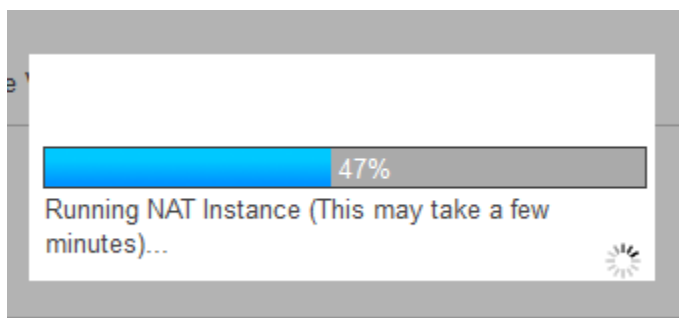
Hardware tenancy:* Default

[Use a NAT gateway instead](#)

Click on Create VPC

[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.

The screenshot displays the AWS VPC Dashboard. On the left, the 'Virtual Private Cloud' section is expanded, with 'Your VPCs' highlighted. A green arrow points to this option. The main area shows a table of VPCs with columns: Name, VPC ID, State, VPC CIDR, DHCP options set, and Route table. Two VPCs are listed: 'demo' (vpc-0c270069) and another (vpc-adfea0c8). The 'demo' VPC is selected and highlighted with a red box. Below the table, the details for 'vpc-0c270069 (10.0.0.0/16) | demo' are shown under the 'Summary' tab. The details include VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, DNS resolution, DNS hostnames, and ClassicLink DNS Support.

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table
demo	vpc-0c270069	available	10.0.0.0/16	dopt-05198260	rtb-819799e4
	vpc-adfea0c8	available	172.31.0.0/16	dopt-05198260	rtb-0ecacb6b

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

Filter by VPC: None

[Create VPC](#) Actions

Search VPCs and their properties

Name	VPC ID	State	VPC CIDR	DHCP
demo	vpc-0c270069	available	10.0.0.0/16	dopt-
	vpc-adfea0c8	available	172.31.0.0/16	dopt-

Select a VPC above

Left Pane:

- Cloud
 - Your VPCs
 - Subnets
 - Route Tables
 - Internet Gateways
 - DHCP Options Sets

Note: A red box highlights 'vpc-0c270069 (10.0.0.0/16) | demo' in the dropdown menu. A green arrow points to the 'demo' row in the table. A pink box contains the text 'Select recently created VPC'.

From left pane select Network ACLs under Security.

VPC Dashboard

Filter by VPC: vpc-0c270069 (10.0.0.0/16)

[Create VPC](#) Actions

Search VPCs and their properties

Name	VPC ID	State	VPC CIDR
demo	vpc-0c270069	available	10.0.0.0/16

Select a VPC above

Left Pane:

- 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

Note: A red box highlights 'Network ACLs' in the left pane. A blue dashed arrow points from a callout box 'Click on Network ACLs' to the 'Network ACLs' item.

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 thei X

<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"
      ]
    }
  ]
}
```

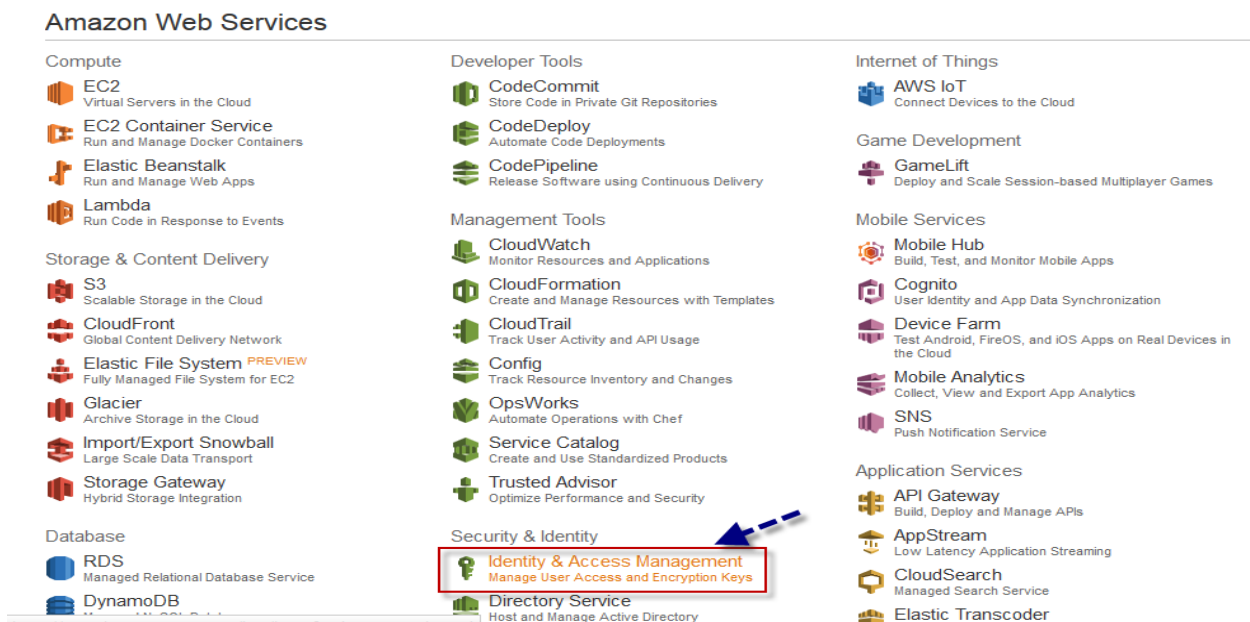
```
    ],  
    "Effect": "Allow",  
    "Resource": "*"    
  }  
]  
}
```

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):

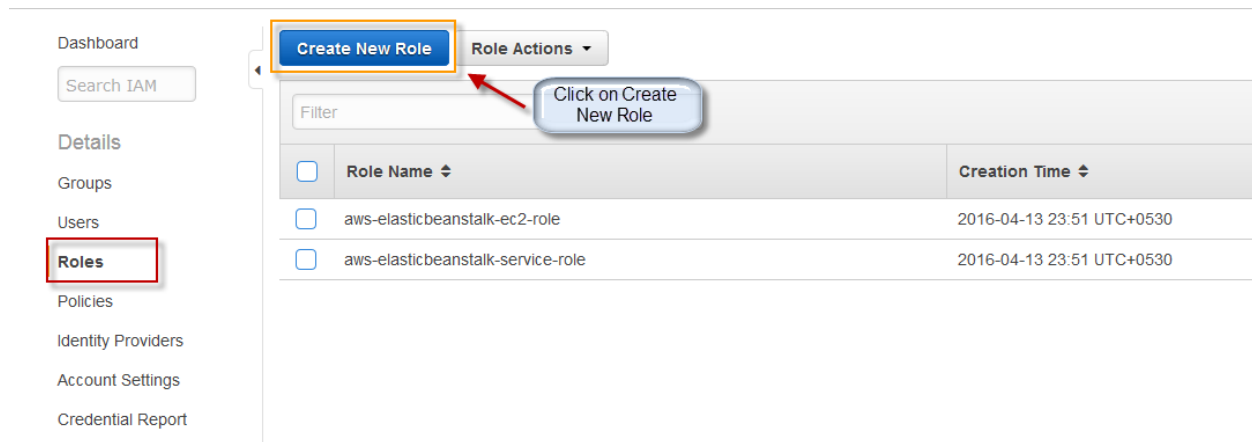
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "",  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "vpc-flow-logs.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

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

Choose Select

Role Name	Description	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 Filter Showing 196 results

Policy Name	Attached Entities	Creation Time	Edited Time
AWSElasticBeanstalkEnhance...	1	2016-02-09 04:47 UTC+0530	2016-02-09 04:47 UTC+0530
AWSElasticBeanstalkMulticont...	1	2016-02-09 04:45 UTC+0530	2016-02-09 04:45 UTC+0530
AWSElasticBeanstalkWebTier	1	2016-02-09 04:38 UTC+0530	2016-03-08 05:05 UTC+0530
AWSElasticBeanstalkWorkerTier	1	2016-02-09 04:42 UTC+0530	2016-03-08 05:08 UTC+0530
AdministratorAccess	0	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+0530
AmazonAPIGatewayAdministra...	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+0530
AmazonAPIGatewayInvokeFull...	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+0530
AmazonAPIGatewayPushToClo...	0	2015-11-12 05:11 UTC+0530	2015-11-12 05:11 UTC+0530
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](#)

[Click here first](#)

Inline Policies

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

[select 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 [Choose Select](#)

☒ **Custom Policy** [Select](#)

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

[Select Custom Policy](#)

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

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.

Select Edit Trust Relationship

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 Amazon EC2 console interface. On the left, the navigation pane is expanded to 'NETWORK & SECURITY', and 'Network Interfaces' is highlighted with a red box and an arrow. The main content area displays the 'Resources' section for the Asia Pacific (Singapore) region, listing various EC2 resources. Below this, there is a 'Create Instance' section with a 'Launch Instance' button. The 'Service Health' and 'Scheduled Events' sections are also visible, showing the status for the Asia Pacific (Singapore) region.

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Singapore) region:

1 Running Instances	1 Elastic IPs
0 Dedicated Hosts	0 Snapshots
2 Volumes	0 Load Balancers
4 Key Pairs	6 Security Groups
0 Placement Groups	

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the Asia Pacific (Singapore) region

Service Health

Service Status:

Asia Pacific (Singapore):

Scheduled Events

Asia Pacific (Singapore):

No events

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 Amazon EC2 console. The 'Actions' dropdown menu is open, and 'Create Flow Log' is highlighted with a red box and an arrow. The table below shows the list of network interfaces.

Create Network Interface **Attach** **Detach** **Delete** **Actions**

Filter by tags and attributes or search by keyword

	Name	Network interf	Subnet ID	VPC	Security groups
<input checked="" type="checkbox"/>	eni-3ed6ca77	eni-3ed6ca77	subnet-4a585b3d	vpc-	default
<input type="checkbox"/>	eni-bf6c8af7	eni-bf6c8af7	subnet-bdebe5ca	vpc-	default

Choose Create Flow Log

Actions

- Attach
- Detach
- Delete
- Manage Private IP Addresses
- Associate Address
- Disassociate Address
- Change Termination Behavior
- Change Security Groups
- Change Source/Dest. Check
- Add/Edit Tags
- Change Description
- 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 →

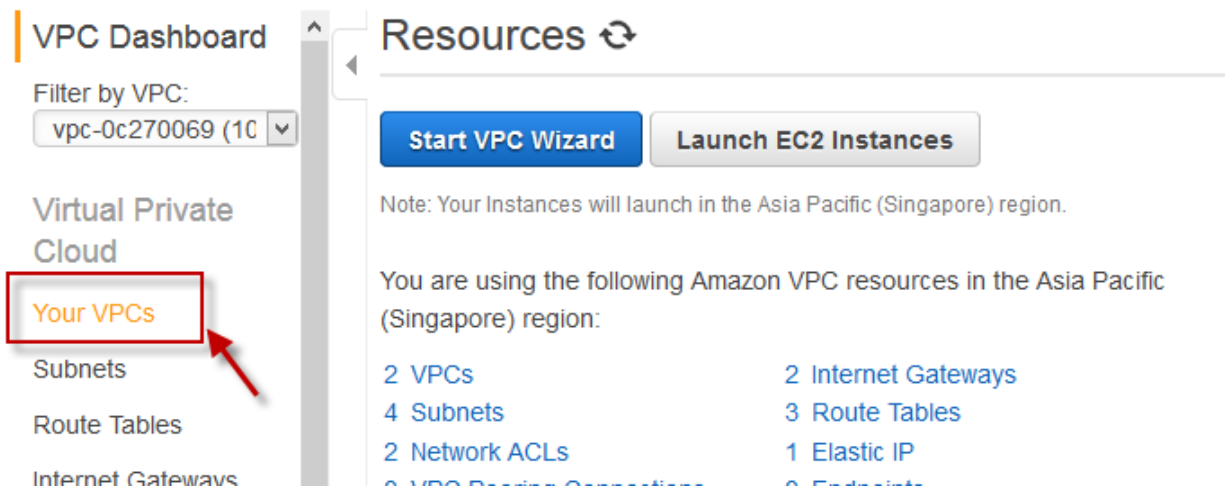
Cancel **Create Flow Log**

*: Required

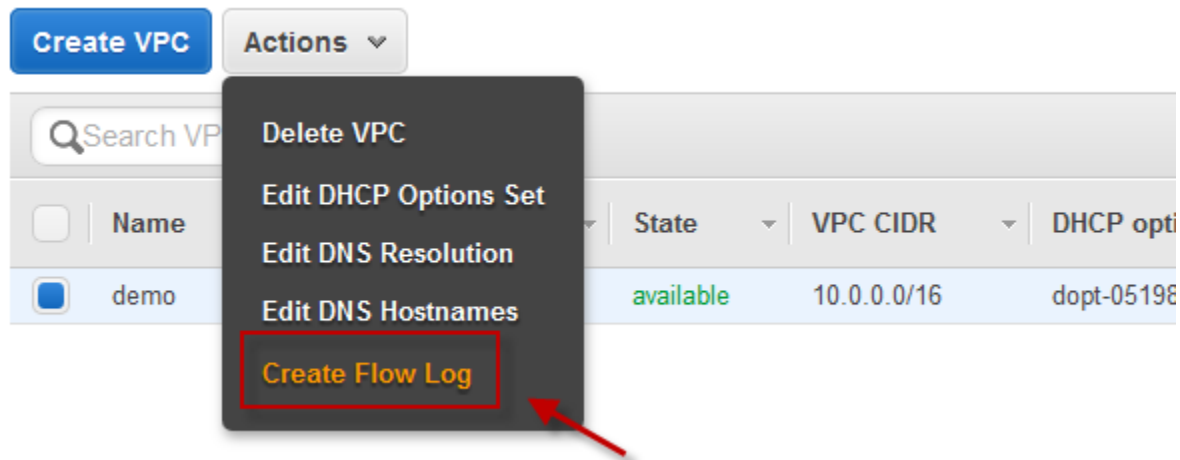
Choose Create Flow Log

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 ?

Annotations:

- Specify a name:** Points to the Destination Log Group field.
- Choose IAM role which created:** Points to the IAM Role dropdown.
- Choose Create Flow Log:** Points to the Create Flow Log button.

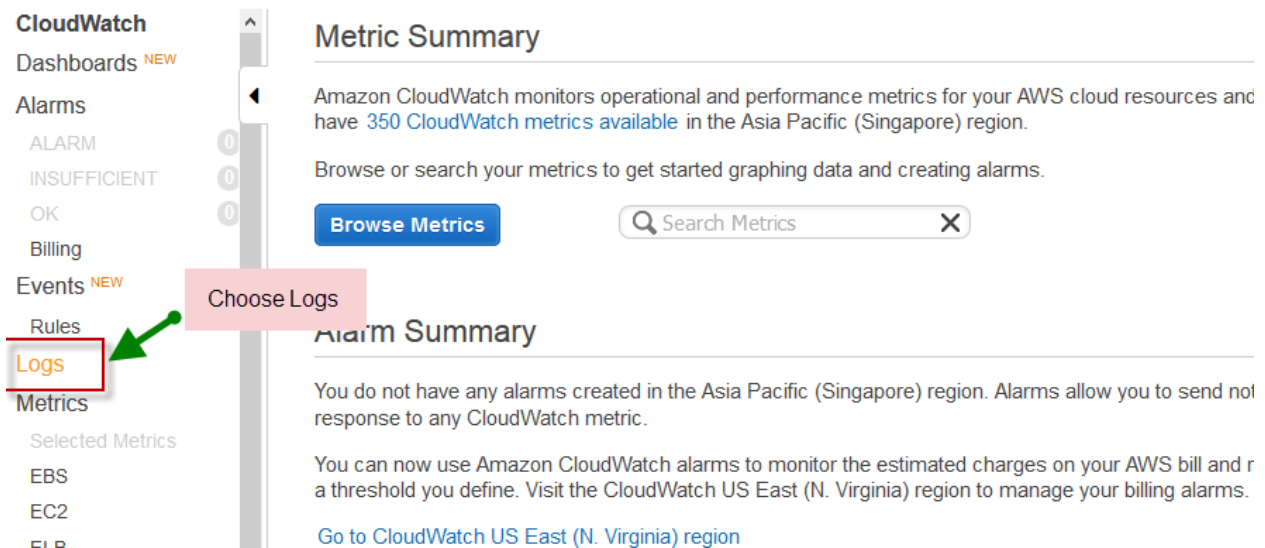
Buttons: Cancel, **Create Flow Log**

*: Required

VIEWING FLOW LOGS

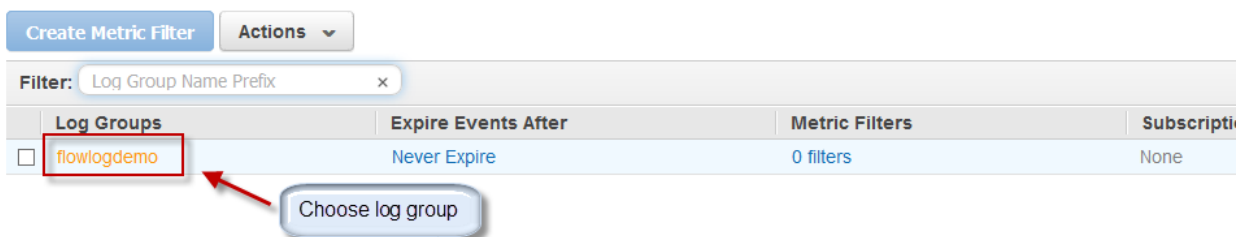
Go to Cloud Watch page from AWS console home.

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 lists various services: CloudWatch, Dashboards, Alarms, Events, Rules, Logs, and Metrics. The 'Logs' option is highlighted with a red box, and a green arrow points to it from a pink callout box labeled 'Choose Logs'. 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 the 'Log Groups' section of the AWS CloudWatch console. At the top, there are buttons for 'Create Metric Filter' and 'Actions'. Below these is a filter input field labeled 'Filter: Log Group Name Prefix'. A table lists the log groups, with columns for 'Log Groups', 'Expire Events After', 'Metric Filters', and 'Subscriptions'. The first row shows a log group named 'flowlogdemo' with a checkbox to its left. A red arrow points from a blue callout box labeled 'Choose log group' to the 'flowlogdemo' entry in the table.

	Log Groups	Expire Events After	Metric Filters	Subscriptions
<input type="checkbox"/>	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:

<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:

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.

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	-	

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**