

1) Create VPC with 2 private and 2 public subnets.

z minutes ago

Find subnets by attribute or tag

< 1 >

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
public-subnet-1	subnet-0573bc9385b3dd19b	Available	vpc-0f0298240c2f5c044 my-vpc	Off	10.0.0.128/28
public-2	subnet-0913b8b08ede1b5be	Available	vpc-0f0298240c2f5c044 my-vpc	Off	10.0.0.144/28
private-subnet-1	subnet-0a1fba61558d010b9	Available	vpc-0f0298240c2f5c044 my-vpc	Off	10.0.0.0/26
private-subnet-2	subnet-05cbbbe034f1859d5	Available	vpc-0f0298240c2f5c044 my-vpc	Off	10.0.0.64/26

2) Enable DNS Hostname in VPC

VPC > Your VPCs > vpc-0f0298240c2f5c044 > Edit VPC settings

VPC details

VPC ID
vpc-0f0298240c2f5c044

Name
my-vpc

DHCP settings

DHCP option set Info

dopt-a15eefc6

DNS settings

Enable DNS resolution Info

Enable DNS hostnames Info

Network Address Usage metrics settings

Enable Network Address Usage metrics Info

3) Enable Auto Assign Public ip in 2 public subnets

VPC > Subnets > subnet-0573bc9385b3dd19b > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID
subnet-0573bc9385b3dd19b

Name
public-subnet-1

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address Info

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info

Enable resource name DNS AAAA record on launch Info

Hostname type Info

Resource name

IP name

VPC > Subnets > subnet-0913b8b08ede1b5be > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID
subnet-0913b8b08ede1b5be

Name
public-2

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address Info

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info

Enable resource name DNS AAAA record on launch Info

Hostname type Info

Resource name

IP name

4) Add 2 private subnets in private route table

rtb-0c9161412dfc4f6d6 / my-private

Actions

Details

Info

Route table ID

rtb-0c9161412dfc4f6d6

VPC

vpc-0f0298240c2f5c044 | my-vpc

Main

No

Owner ID

147834559194

Explicit subnet associations

2 subnets

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (2)

Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
private-subnet-1	subnet-0a1fba61558d010b9	10.0.0.0/26	-
private-subnet-2	subnet-05cbbbe034f1859d5	10.0.0.64/26	-

Subnets without explicit associations (0)

Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
------	-----------	-----------	-----------

5) Add 2 public subnets in public route table

rtb-03d8f0d8cebe8f2bb

Actions

Details

Info

Route table ID

rtb-03d8f0d8cebe8f2bb

VPC

vpc-0f0298240c2f5c044 | my-vpc

Main

Yes

Owner ID

147834559194

Explicit subnet associations

2 subnets

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (2)

Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
public-subnet-1	subnet-0573bc9385b3dd19b	10.0.0.128/28	-
public-2	subnet-0913b8b08ede1b5be	10.0.0.144/28	-

Subnets without explicit associations (0)

Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
------	-----------	-----------	-----------

6) Public route table will have the routes to internet and local

rtb-03d8f0d8cebe8f2bb / public

Actions

Details

Info

Route table ID

rtb-03d8f0d8cebe8f2bb

VPC

vpc-0f0298240c2f5c044 | my-vpc

Main

Yes

Owner ID

147834559194

Explicit subnet associations

2 subnets

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-09b72676fe42a4615	Active	No
10.0.0.0/24	local	Active	No

7) Create Ec2 in public subnet with t2micro and install php

```
[root@ip-10-0-0-140 ec2-user]# php -v
PHP 5.4.16 (cli) (built: Apr 7 2025 16:22:27)
Copyright (c) 1997-2013 The PHP Group
Zend Engine v2.4.0, Copyright (c) 1998-2013 Zend Technologies
[root@ip-10-0-0-140 ec2-user]#
```

8) COnfigure Nat gateway in public subnet and connect to private Instance

Configured nat gateway in public subnet and connected to private instance

Public machine 10.0.0.140 for this machine logged in to 10.0.0.7 private machine and from that private machine pinging google.com

```
[ec2-user@ip-10-0-0-140 ~]$ ssh -i key.pem ec2-user@10.0.0.7
Last login: Mon Jun  9 12:20:39 2025 from ip-10-0-0-140.us-west-2.compute.internal

#_
#####      Amazon Linux 2
#####\
#####|      AL2 End of Life is 2026-06-30.
#####/
#/_
V~' '->
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-0-7 ~]$ ping google.com
PING google.com (142.251.215.238) 56(84) bytes of data:
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=1 ttl=116 time=7.84 ms
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=2 ttl=116 time=6.58 ms
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=3 ttl=116 time=6.99 ms
64 bytes from sea09s35-in-f14.1e100.net (142.251.215.238): icmp_seq=4 ttl=116 time=7.52 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 6.582/7.237/7.846/0.493 ms
[ec2-user@ip-10-0-0-7 ~]$
```

9) Install Apache Tomcat in private ec2 and deploy a sample app.

```
[root@ip-10-0-0-7 tomcat]# cd webapps/
[root@ip-10-0-0-7 webapps]# wget https://tomcat.apache.org/tomcat-9.0-doc/appdev/sample/sample.war
--2025-06-09 12:47:50-- https://tomcat.apache.org/tomcat-9.0-doc/appdev/sample/sample.war
Resolving tomcat.apache.org (tomcat.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to tomcat.apache.org (tomcat.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4606 (4.5K)
Saving to: 'sample.war'

100%[=====>] 4,606 --.-K/s in 0s

2025-06-09 12:47:50 (30.0 MB/s) - 'sample.war' saved [4606/4606]

[root@ip-10-0-0-7 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample.war
[root@ip-10-0-0-7 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample  sample.war
[root@ip-10-0-0-7 webapps]# ls
docs  examples  host-manager  manager  ROOT  sample  sample.war
[root@ip-10-0-0-7 webapps]# clear
[root@ip-10-0-0-7 webapps]# curl http://localhost:8080/sample/
<html>
<head>
<title>Sample "Hello, World" Application</title>
</head>
<body bgcolor=white>

<table border="0">
<tr>
<td>

</td>
<td>
<h1>Sample "Hello, World" Application</h1>
<p>This is the home page for a sample application used to illustrate the
source directory organization of a web application utilizing the principles
outlined in the Application Developer's Guide.
</td>
</tr>
</table>

<p>To prove that they work, you can execute either of the following links:
<ul>
<li>To a <a href="hello.jsp">JSP page</a>.
<li>To a <a href="hello">servlet</a>.
</ul>

</body>
</html>
[root@ip-10-0-0-7 webapps]#
```

10) Configure VPC flow logs and store the logs in s3 and cloudwatch.

Log groups (1)

By default, we only load up to 10000 log groups.

Filter log groups or try prefix search

Exact match

Log group

Log class

Anomaly d...

Data pr...

Sensitiv...

Retention

Metric fi

aslamlog

Standard

Configure

-

-

Never expire

-

Logs Insights

Info

Start tailing

Select log groups, and then run a query or [choose a sample query](#).

Logs Insights QL

OpenSearch PPL - new

OpenSearch SQL - new

30m

3h

1h

Compare (Off)

UTC timezone

Select log groups by

Log group name

Selection criteria

Select up to 50 log groups

aslamlog

Clear all

Browse log groups

1 fields @timestamp, @message, @logStream, @Log

2 | sort @timestamp desc

3 | limit 10000

Query generator

Run query

Cancel

Save

History

Logs Insights QL query can run for maximum of 60 minutes.

Discovered fields

Saved and sample queries

Query commands

arn:aws:logs:us-west-2:147834559194:log-group:aslamlog:*

0

-

Creation time

2 minutes ago

Retention

Never expire

Stored bytes

-

Contributor Insights rules

-

KMS key ID

-

Anomaly detection

Configure

Field indexes

Configure

Transformer

Configure

Log streams

Tags

Anomaly detection

Metric filters

Subscription filters

Contributor Insights

Data protection

Field in

Log streams (3)

Delete

Create log stream

Search all log streams

Filter log streams or try prefix search

Exact match

Show expired

Info

Log stream

Last event time

eni-093dd7aa5fb2a0807-all

2025-06-09 13:06:43 (UTC)

eni-0466aa63b6f32830e-all

2025-06-09 13:06:00 (UTC)

eni-008f15a83c8ec78a1-all

2025-06-09 13:05:16 (UTC)