

VPC Task -1

1. Created VPC with 2 private and 2 public subnets.

The screenshot shows two tables from the AWS VPC console. The top table lists VPCs with one entry: "my-vpc" (VPC ID: vpc-0277d18e91aa78b45, State: Available). The bottom table lists subnets with four entries:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
public-subnet-2	subnet-03ca7dc51a3996af4	Available	vpc-0277d18e91aa78b45 my-vpc	Off	198.168.2.0/24
Public-subnet-1	subnet-08b26f68db3efb950	Available	vpc-0277d18e91aa78b45 my-vpc	Off	198.168.1.0/24
private-subnet-2	subnet-004502991cfb4e6e1	Available	vpc-0277d18e91aa78b45 my-vpc	Off	198.168.4.0/24
private-subnet-1	subnet-09fd33rhdha2313f	Available	vnr-0277d18e91aa78b45 my-vpc	Off	198.168.3.0/24

Select a subnet

2. Enabled DNS Hostname in VPC.

- Enabled the dns resolution and dns hostname.
- I went to vpc > actions > vpc settings > then enable DNS

The screenshot shows the "Edit VPC settings" page for "my-vpc". Under "DNS settings", the checkboxes "Enable DNS resolution" and "Enable DNS hostnames" are checked.

3. Enable Auto Assign Public IP in 2 public subnets.

The screenshot shows the "Edit subnet settings" page for "Public-subnet-1". Under "Auto-assign IP settings", the checkbox "Enable auto-assign public IPv4 address" is checked. The note below states: "Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet."

Edit subnet settings Info**Subnet**

Subnet ID
[subnet-03ca7dc51a3996af4](#)

Name
[public-subnet-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**4. Add 2 private subnets in private route table.**

- I went to rout table < create private root < subnet < edit subnet association < add private subnet.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
private-subnet-1	subnet-096d33cb6dba2313f	198.168.3.0/24	-
private-subnet-2	subnet-004502991cfb4e6e1	198.168.4.0/24	-

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Public-subnet-1	subnet-08b26f68db3efb950	198.168.1.0/24	-
public-subnet-2	subnet-03ca7dc51a3996af4	198.168.2.0/24	-

5. Add 2 public subnets in public route table.

- I went to rout table < create public root < subnet < edit subnet association < add public subnet.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Public-subnet-1	subnet-08b26f68db3efb950	198.168.1.0/24	-
public-subnet-2	subnet-03ca7dc51a3996af4	198.168.2.0/24	-

No subnets without explicit associations

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

- Created new internetgateway for my vpc
- opened **Edit routes** for the public-route table.
- verified the **local route (198.168.0.0/16 → local)** which AWS added automatically.
- then **added a new route (0.0.0.0/0 → your Internet Gateway igw-0be596178cec47331)** to enable

VPC > Route tables > rtb-0a8fb6ef8cd6b758b > Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin
198.168.0.0/16	local	Active	No	CreateRouteTable
Q 0.0.0.0/0	Internet Gateway	In Progress	No	CreateRoute
	Q igw-0be596178cec47331	Pending	No	CreateRouteTable

Add route

Use: "igw-0be596178cec47331"
igw-0be596178cec47331 (my-internet-gateway)

Cancel Preview Save changes

7. Create EC2 in public subnet with t2.micro and install PHP.

-

EC2 > Instances > i-028f17a283b09fa61

Instance summary for i-028f17a283b09fa61 (Server_with_VPC) [Info](#) [Connect](#) [Instance state](#) [Actions](#)

Updated less than a minute ago

Instance ID i-028f17a283b09fa61	Public IPv4 address 44.202.223.145 open address	Private IPv4 addresses 198.168.1.17
IPv6 address -	Instance state Running	Public DNS ec2-44-202-223-145.compute-1.amazonaws.com open address
Hostname type IP name: ip-198-168-1-17.ec2.internal	Private IP DNS name (IPv4 only) ip-198-168-1-17.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address 44.202.223.145 [Public IP]	VPC ID vpc-0277d18e91aa78b45 (my-vpc)	Learn more Activate Windows Go to Settings to activate Windows.

Not secure 44.202.223.145

YouTube News Maps Translate Google Data Science Mind...

PHP Version 8.4.14



System	Linux ip-198-168-1-17 ec2 internal 6.1.158-178.288.amzn2023.x86_64 #1 SMP PREEMPT_DYNAMIC Mon Nov 3 18:38:36 UTC 2025 x86_64
Build Date	Oct 21 2025 19:23:55
Build System	Linux
Build Provider	Amazon Linux
Compiler	gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-5)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/0-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-crypt.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-eaxini, /etc/php.d/20-fileno.ini, /etc/php.d/20-fp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlind.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-pecl.ini, /etc/php.d/20-shmop.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sodium.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-sysvmsg.ini, /etc/php.d/20-sysvsem.ini, /etc/php.d/20-sysvshm.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmreader.ini
PHP API	20240924
PHP Extension	20240924
Zend Extension	420240924
Zend Extension Build	API20240924.NTS
PHP Extension Build	API20240924.NTS
PHP Integer Size	64 bits
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled

Activate Window
Go to Settings to activate

```

Verifying : php8.4-mysqlind-8.4.14-1.amzn2023.0.1.x86_64
Verifying : php8.4-opcache-8.4.14-1.amzn2023.0.1.x86_64
Verifying : php8.4-pdo-8.4.14-1.amzn2023.0.1.x86_64
Verifying : php8.4-process-8.4.14-1.amzn2023.0.1.x86_64
Verifying : php8.4-sodium-8.4.14-1.amzn2023.0.1.x86_64
Verifying : php8.4-xml-8.4.14-1.amzn2023.0.1.x86_64

Installed:
  apr-1.7.5-1.amzn2023.0.4.x86_64          apr-util-1.6.3-1.amzn2023.0.2.x86_64        apr-util-lmdb-1.6.3-1.amzn2023.0.2.x86_64      apr-util-openssl-1.6.3-1.amzn2023.0.2.x86_64    httpd-2.4.65-1.amzn2023.0.2.x86_64
  httpd-filesystem-0.65-1.amzn2023.0.2.noarch httpd-tools-2.4.65-1.amzn2023.0.2.x86_64      libbrotli-1.0.9-4.amzn2023.0.2.x86_64        libodium-1.0.19-4.amzn2023.x86_64            libxml-1.1.43-1.amz
  mod_http2-2.0.27-1.amzn2023.0.3.x86_64     mod_lua-2.4.65-1.amzn2023.0.2.x86_64        libphb-8.4-8.4.14-1.amzn2023.0.1.x86_64       php8.4-common-8.4.14-1.amzn2023.0.1.x86_64   php8.4-xml-8.4.14-1.amzn2023.0.1.x86_64
  php8.4-mysqlind-8.4.14-1.amzn2023.0.1.x86_64 php8.4-opcache-8.4.14-1.amzn2023.0.1.x86_64      php8.4-pdo-8.4.14-1.amzn2023.0.1.x86_64       php8.4-process-8.4.14-1.amzn2023.0.1.x86_64

Complete!
[ec2-user@ip-198-168-1-17 ~]$ php -v
PHP 8.4.14 (cli) (built: Oct 21 2025 19:23:55) (NTS gcc x86_64)
Copyright (c) The PHP Group
Built by Amazon Linux
Zend Engine v4.4.14 Copyright (c) Zend Technologies
  - Zend Script Engine v4.4.14 Copyright (c) by Zend Technologies
[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl start php-fpm
sudo systemctl enable php-fpm
Created symlink /etc/systemd/system/multi-user.target.wants/php-fpm.service → /usr/lib/systemd/system/php-fpm.service.
[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl status php-fpm
● php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php-fpm.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-11-21 12:59:21 UTC; 31s ago
     Main PID: 26597 (php-fpm)
    Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0.00req/sec"
      Tasks: 6 (limit: 1106)
     Memory: 10.3M
        CPU: 50ms
       CGroup: /system.slice/php-fpm.service
           └─ 26597 php-fpm: master process (/etc/php-fpm.conf)

Nov 21 12:59:21 ip-198-168-1-17.ec2.internal systemd[1]: Starting php-fpm.service - The PHP FastCGI Process Manager...
Nov 21 12:59:21 ip-198-168-1-17.ec2.internal systemd[1]: Started php-fpm.service - The PHP FastCGI Process Manager.
[ec2-user@ip-198-168-1-17 ~]$ sudo name /etc/nginx/nginx.conf
[ec2-user@ip-198-168-1-17 ~]$ sudo vi /etc/nginx/nginx.conf
[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl restart nginx
[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl php-fpm
Unknown command: verify_phpfpm.

[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl start php-fpm
[ec2-user@ip-198-168-1-17 ~]$ echo "<?php phpfpm(); ?>" | sudo tee /var/www/html/index.php
<?php phpfpm(); ?>
[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl restart nginx
[ec2-user@ip-198-168-1-17 ~]$ sudo systemctl restart php-fpm
[ec2-user@ip-198-168-1-17 ~]$ cd root /usr/share/nginx/html;
-bash: cd: command not found
[ec2-user@ip-198-168-1-17 ~]$ root /usr/share/nginx/html
-bash: root: command not found
[ec2-user@ip-198-168-1-17 ~]$ cd root /usr/share/nginx
-bash: cd: too many arguments
[ec2-user@ip-198-168-1-17 ~]$ cd root /usr/share/nginx/
-bash: cd: too many arguments
[ec2-user@ip-198-168-1-17 ~]$ cd /usr/share/nginx/
[ec2-user@ip-198-168-1-17 nginx]$ ls
html modules
[ec2-user@ip-198-168-1-17 nginx]$ vi html
[ec2-user@ip-198-168-1-17 nginx]$ sudo mv /var/www/html/index.php /usr/share/nginx/html/index.php
[ec2-user@ip-198-168-1-17 nginx]$ sudo rm -f /usr/share/nginx/html/index.html
[ec2-user@ip-198-168-1-17 nginx]$ sudo systemctl restart php-fpm
sudo systemctl restart nginx
[ec2-user@ip-198-168-1-17 nginx]$ |

```

8. Configure NAT gateway in public subnet and connect to private instance.

I created an Elastic IP

You must allocate a new Elastic IP:

AWS Console > **VPC** > **Elastic IPs** → Allocate.

I created a NAT Gateway in the Public Subnet

AWS Console > **VPC** > **NAT Gateways** > Create NAT Gateway

Choose:

- **Subnet** → Any *public* subnet
- **Elastic IP** → Select the one you allocated
- **Name** → nat-gw

Click **Create NAT Gateway**

I updated the Private Route Table

Go to:

VPC → **Route Tables** → Select the private route table

Then:

Route → **0.0.0.0/0**

Target → **NAT Gateway (nat-gw-xxxx)**

Click **Save Changes**

This ensures ALL private instances route outbound traffic through the NAT Gateway.

I confirmed private subnets are associated with Private Route Table

Under the same route table:

- Subnet associations →
Both **private-subnet-1** and **private-subnet-2** must be selected.
-

I launched an EC2 instance in Private Subnet

You will now:

- Launch instance
 - Choose **private subnet**
 - Auto-assign public IP = **Disabled**
 - Security Group → allow SSH only from the public EC2 (optional)
-

I verified private instance can access Internet (via NAT Gateway)

SSH to public EC2:

ssh -i key.pem ec2-user@<public-ec2-ip>

Then from public EC2, SSH to private EC2:

ssh ec2-user@<private-ec2-ip>

Test internet:

ping google.com

sudo yum install git -y

NAT gateway nat-0556ad570496eab19 | my_natget was created successfully.

nat-0556ad570496eab19 / my_natget

Actions

Details			
NAT gateway ID nat-0556ad570496eab19	Connectivity type Public	State Pending	State message Info -
NAT gateway ARN arn:aws:ec2:us-east-1:679625722057:natgateway/nat-0556ad570496eab19	Primary public IPv4 address -	Primary private IPv4 address -	Primary network interface ID -
VPC vpc-0277d18e91aa78b45 / my-vpc	Subnet subnet-08b26f68db3efb950 / Public-subnet-1	Created Saturday, November 22, 2025 at 16:34:39 GMT+5:30	Deleted -

Secondary IPv4 addresses [Monitoring](#) [Tags](#)

Secondary IPv4 addresses

[Edit secondary IPv4 address associations](#)

Activate Windows [Go to Settings to activate Windows](#)

Resource map [CIDRs](#) [Flow logs](#) [Tags](#) [Integrations](#)

Resource map [Info](#)

Show all details

```

graph LR
    nets["nets (4)"]
    publicRoute["public-route"]
    privateRT["Private-rt"]
    myInternetGateway["my-internet-gateway"]
    myNatGet["my_natget"]

    nets --- publicRoute
    nets --- privateRT
    publicRoute --- myInternetGateway
    publicRoute --- myNatGet
    privateRT --- myInternetGateway
    privateRT --- myNatGet
  
```

-----BEGIN RSA PRIVATE KEY-----
MIIowIBAAKCAgQAwIIDNFn7WfdriJ3uAebiy5Y4ASYQ2JGVYRkgBlaZzB
...
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAgQAwIIDNFn7WfdriJ3uAebiy5Y4ASYQ2JGVYRkgBlaZzB
...
-----END RSA PRIVATE KEY-----

Arjumand@Arjumand MINGW64 ~/Downloads (master)

```

$ ssh -T ec2-user@198.168.1.55
The authenticity of host '3.227.16.75 (3.227.16.75)' can't be established.
ED25519 key fingerprint is SHA256:C4SEjJrNRuUVFAvtBtRVA3EjL47RmvktpCU0c59p4wQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.227.16.75' (ED25519) to the list of known hosts.
# 
# Amazon Linux 2023
## 
## https://aws.amazon.com/linux/amazon-linux-2023
## 
## 
## 
## 
[ec2-user@ip-198-168-1-55 ~]$ ls
[ec2-user@ip-198-168-1-55 ~]$ vi private.pem
[ec2-user@ip-198-168-1-55 ~]$ chmod 400 private.pem
[ec2-user@ip-198-168-1-55 ~]$ ssh -i private.pem ec2-user@198.168.3.186
The authenticity of host '198.168.3.186 (198.168.3.186)' can't be established.
ED25519 key fingerprint is SHA256:NyTEmrsVs0tgJk7Izs1jWApsmkTmSeJDHghZhA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '198.168.3.186' (ED25519) to the list of known hosts.
# 
# Amazon Linux 2023
## 
## https://aws.amazon.com/linux/amazon-linux-2023
## 
## 
## 
## 
[ec2-user@ip-198-168-3-186 ~]$ 

```

- Connected to private instance successfully.

9. Install Apache Tomcat in private EC2 and deploy a sample app.

- **Connected to Private EC2 through Public EC2**
- SSH → public instance
- From there SSH → private instance (jump host method)
- ---
- **2. Installed Java and Set Up Tomcat**
- Downloaded Tomcat, extracted to /opt/tomcat
- Created tomcat user
- Gave ownership:
- sudo chown -R tomcat: /opt/tomcat
- ---
- **3. Fixed the Permission Issue (bin Folder Not Opening)**
- You were stuck entering the bin folder.
You fixed it using:
- sudo chmod -R 755 /opt/tomcat/bin
- Then successfully ran:
- cd /opt/tomcat/bin
- ---
- **4. Created Tomcat Systemd Service & Started Tomcat**
- sudo systemctl daemon-reload
- sudo systemctl start tomcat
- sudo systemctl enable tomcat
- ---
- **5. Deployed a Simple Test App**
- Created a simple JSP app:
- echo "<h1>Hello from Tomcat!</h1>" | sudo tee /opt/tomcat/webapps/ROOT/test.jsp
- ---
- **6. Verified Using curl from Public Instance**
- You tested the app:
- curl http://<private-ec2-ip>:8080/test.jsp

```
50 sudo wget https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.112/bin/apache-tomcat-9.0.112.tar.gz
51 ls
52 rm tomcat
53 sudo rm tomcat
54 sudo tar -xvzf apache-tomcat-9.0.112.tar.gz
55 mv apache-tomcat-9.0.112 tomcat9
56 sudo mv apache-tomcat-9.0.112 tomcat9
57 sudo chown -R tomcat:tomcat9 tomcat9
58 cd tomcat9
59 ls
60 sudo cd bin
61 ll
62 sudo bin/
63 sudo cd bin/
64 sudo cd /bin
65 cd bin
66 sudo cd bin
67 cd webapps
68 cd webapps
69 sudo cd webapps
70 sudo chmod 755 ec2-user:ec2-user /opt/tomcat9
71 cd /opt/tomcat9
72 ls -l
73 cd bin
74 ./startup.sh
75 cd /opt/tomcat9/webapps
76 sudo wget https://tomcat.apache.org/tomcat-9.0-doc/appdev/sample/sample.war
77 cd /opt/tomcat9/bin
78 ./shutdown.sh
79 sudo ./startup.sh
80 curl http://198.168.3.186:8080/sample/
```

Activate
Go to Settings

```
[root]---- Z ec2-user ec2-user 31 Nov 8 07:46 webapps
[root]---- Z ec2-user ec2-user 31 Nov 6 07:46 work
[ec2-user@ip-198-168-3-186 bin]$ cd /opt/tomcat9
Using CATALINA_BASE:   /opt/tomcat9
Using CATALINA_HOME:  /opt/tomcat9
Using CATALINA_TMPDIR: /opt/tomcat9/temp
Using CLASSPATH:       /opt/tomcat9/bin/bootstrap.jar:/opt/tomcat9/bin/tomcat-juli.jar
Using CATALINA_OPTS:
[ec2-user@ip-198-168-3-186 bin]$ cd /opt/tomcat9/webapps
[ec2-user@ip-198-168-3-186 webapps]$ sudo wget https://tomcat.apache.org/tomcat-9.0-doc/appdev/sample/sample.war
--2023-11-22 18:07:05 -- [  0.00K /  1.00M] 100%[=] 00:00:00 ETA
Resolving tomcat.apache.org (tomcat.apache.org)... 151.101.2.132, 2a04:4e21:644
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'

sample.war                                              100%[=] 4606/4606
2023-11-22 18:07:05 (8.3 MB/s) - 'sample.war' saved [4606/4606]

[ec2-user@ip-198-168-3-186 webapps]$ cd /opt/tomcat9/bin
[ec2-user@ip-198-168-3-186 bin]$ ./shutdown.sh
Using CATALINA_BASE:   /opt/tomcat9
Using CATALINA_HOME:  /opt/tomcat9
Using CATALINA_TMPDIR: /opt/tomcat9/temp
Using CATALINA_OPTS:
Using CATALINA_OPTS: -Dcatalina.home=/opt/tomcat9
Using CATALINA_OPTS: -Dcatalina.base=/opt/tomcat9
Using CATALINA_OPTS: -Dcatalina.tmpdir=/opt/tomcat9/temp
Using CATALINA_OPTS: -Dcatalina.basedir=/opt/tomcat9
Using CATALINA_OPTS: -Djava.util.logging.config.file=logging.properties
Using CLASSPATH:       /opt/tomcat9/bin/bootstrap.jar:/opt/tomcat9/bin/tomcat-juli.jar
Using CATALINA_OPTS:
[ec2-user@ip-198-168-3-186 bin]$ curl http://198.168.3.186:8080/sample/
<!DOCTYPE html>
<html>
<head>
<title>Sample "Hello, World" Application</title>
<style>body{color:white; background-color:black;}</style>
</head>
<body>
<h2>Hello, World!</h2>
<p>The following page illustrates the basic organization used to illustrate the source directory organization of a web application utilizing the principles outlined in the Application Developer's Guide.</p>
</body>
</html>

```

10. Configure VPC flow logs and store the logs in S3 and CloudWatch.

Steps:

1. Go to VPC Console, select your VPC (project-vpc), and open the Flow Logs tab.
 2. Click Create flow log and enter the name: vpc-flowlogs-cw.
 3. Set Filter = All and Aggregation Interval = 1 or 10 minutes.
 4. Choose Destination → CloudWatch Logs, then create a new log group:
/vpc/flowlogs/project-vpc
 5. Under Service Access, click Set up permissions → let AWS create a new IAM role → select that role.
 6. Click Create flow log and CloudWatch will start receiving VPC traffic logs.

Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

Accept
 Reject
 All

Maximum aggregation interval | [Info](#)
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

10 minutes
 1 minute

Destination
The destination to which to publish the flow log data.

Send to CloudWatch Logs
 Send to an Amazon S3 bucket
 Send to Amazon Data Firehose in the same account
 Send to Amazon Data Firehose in a different account

Destination log group | [Info](#)
The name of an existing log group or the name of a new log group that will be created when you create this flow log. A new log stream is created for each monitored network interface.

/vpc/flowlogs/project-vpc [X](#)

Service access
VPC flow logs require permissions to create log groups and publish events in CloudWatch.

Use an existing service role
 Create and use a new service role

Service role name | [Info](#)
 VPCFlowLogs-Cloudwatch-1763835908259

Log record format
Specify the fields to include in the flow log record.

AWS default format
 Custom format

Additional metadata
Include additional metadata to AWS default log record format.

Include Amazon ECS metadata

Format preview

```
 ${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

 Name [X](#)

Value - optional

 vpc-flowlog-cw

[Add tag](#)

You can add 49 more tags

Log group details

Log class Info	Metric filters 0	Sensitive data count -
Standard	Subscription filters 0	Custom field indexes Configure
ARN arn:aws:logs:us-east-1:679625722057:log-group:/vpc/flowlogs/project-vpc*	Contributor Insights rules -	Transformer Configure
Creation time 28 minutes ago	KMS key ID -	Anomaly detection Configure
Retention Never expire	Data protection -	
Stored bytes -		

Log streams | Tags | Anomaly detection | Metric filters | Subscription filters | Contributor Insights | Data protection | Field indexes | Transformer

Log streams (3)

By default, we only load the most recent log streams.

<input type="checkbox"/> Log stream	Last event time
<input type="checkbox"/> eni-0609b13d080ad3d1-all	2025-11-22 18:40:55 (UTC)
<input type="checkbox"/> eni-0f08d635dce95ca9-all	2025-11-22 18:40:37 (UTC)
<input type="checkbox"/> eni-051cde8d7283aa41e-all	2025-11-22 18:38:21 (UTC)

[Create log stream](#) | [Search all log streams](#)

Activate Windows
Go to Settings to activate Windows.

VPC Flow Logs to S3 — Simple 7 Steps

1. Create an S3 bucket (example: mmyflowlog-s3)
2. Copy the bucket ARN from S3 → Properties (example: arn:aws:s3:::mmyflowlog-s3)
3. Go to VPC → Your VPCs → Flow Logs → Create flow log
4. Set Filter = All and Aggregation = 10 minutes
5. Choose Destination = Send to Amazon S3 bucket
6. Paste your S3 bucket ARN and keep default log format
7. Click Create flow log — DONE

New Bucket created:

[fl-0c89d5e5e649f9b2a / flowlog-s3](#) | [Actions ▾](#)

Details

Flow Log ID fl-0c89d5e5e649f9b2a	Destination Type s3	Traffic Type All	File Format Plain text
Name flowlog-s3	Destination Name mmyflowlog-s3	Max Aggregation Interval 10 minutes	Hive Compatible Partitions Not enabled
State Active	IAM Role -	Log Format Default	Partition Logs Daily
Creation Time Sunday, November 23, 2025 at 00:29:52 GMT+5:30	Cross Account IAM Role -		

Tags | [Integrations](#)

Tags

Key	Value
Name	flowlog-s3

[Manage tags](#)

Filter

The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

- Accept
- Reject
- All

Maximum aggregation interval | [Info](#)

The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

- 10 minutes
- 1 minute

Destination

The destination to which to publish the flow log data.

- Send to CloudWatch Logs
- Send to an Amazon S3 bucket
- Send to Amazon Data Firehose in the same account
- Send to Amazon Data Firehose in a different account

S3 bucket ARN

The ARN of the Amazon S3 bucket to which the flow log is published. You can specify a specific folder in the bucket using the arn:aws:s3:::prefix

[S3 bucket ARN...](#)

Must be in the format: arn:aws:s3:::[bucket-name]

(i) Please note, a resource-based policy will be created for you and attached to the target bucket.

Log record format

Specify the fields to include in the flow log record.

- AWS default format
- Custom format

Additional metadata

Include additional metadata to AWS default log record format.

- Include Amazon ECS metadata

Format preview

`${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes}`

mmyflowlog-s3 [Info](#)

[Objects](#) | [Metadata](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (1)

Objects are fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	AWSLogs/	Folder	-	-	-