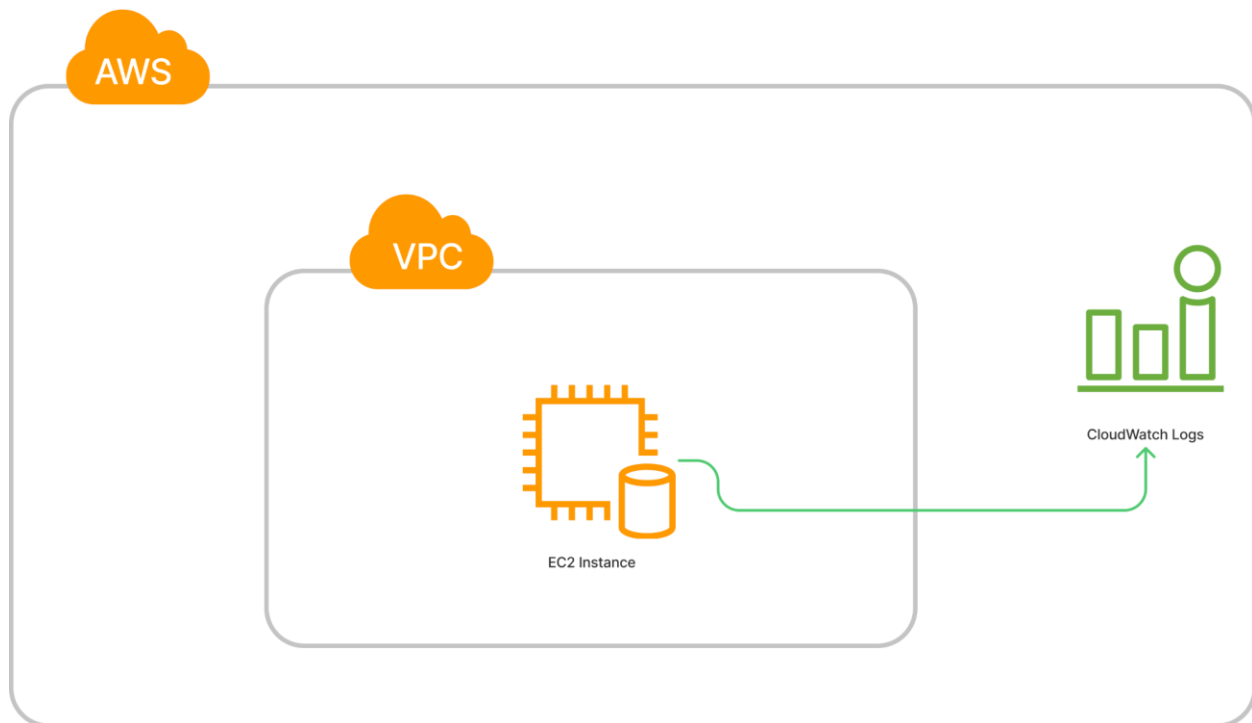


Ques 1: Follow Up the below AWS Architecture Diagram and Create the same in AWS, after created store the store the cloudwatch logs in the **logs.txt** file.



Solution:

- **Creating VPC for EC2:**

The screenshot shows the AWS Management Console interface. A green banner at the top states: "You successfully created vpc-0a39e34261d4eaba3 / MyVpc". The main content area displays the details for the VPC `vpc-0a39e34261d4eaba3 / MyVpc`. The details are organized into a table with four columns: VPC ID, State, DNS hostnames, and DNS resolution.

VPC ID	State	DNS hostnames	DNS resolution
<code>vpc-0a39e34261d4eaba3</code>	Available	Disabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	<code>dopt-0e46ed8a935e80940</code>	<code>rtb-017ed258160968496</code>	<code>acl-07c9b29dba14d9688</code>
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
No	<code>10.0.0.0/16</code>	-	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	
Disabled	-	<code>607897239025</code>	

Below the details table, there are tabs for "Resource map", "CIDRs", "Flow logs", and "Tags". The "Resource map" tab is selected, showing a visual representation of the VPC resources, including subnets, route tables, and network connections.

• Creating Subnet For EC2:

Subnets (1) info

Subnet ID: subnet-0e45f1c450b8fb448

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
mysubnet-1	subnet-0e45f1c450b8fb448	Available	vpc-0a39e34261d4eaba3 My...	10.0.1.0/24	-

Select a subnet

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

• Creating Internet Gateway:

Create internet gateway info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
myInternetGateway

Tags - optional
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 Value - optional: myInternetGateway

Add new tag

You can add 49 more tags.

Cancel Create internet gateway

Internet gateway igw-04328724e6eb5811c successfully attached to vpc-0a39e34261d4eaba3

VPC > Internet gateways > igw-04328724e6eb5811c

igw-04328724e6eb5811c / myInternetGateway

Details info

Internet gateway ID igw-04328724e6eb5811c	State Attached	VPC ID vpc-0a39e34261d4eaba3 MyVpc	Owner 607897239025
--	-------------------	---	-----------------------

Tags

Search tags

Key	Value
Name	myInternetGateway

Manage tags

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- Creating Route table:

rtb-017ed258160968496

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Details

Route table ID rtb-017ed258160968496	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-0a39e34261d4eaba3 MyVpc	Owner ID 607897239025		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-04328724e6eb5811c	Active	No
10.0.0.0/16	local	Active	No

- Ec2 created:

Instance summary for i-0fb1e65047d86c419 (MyVm)

Updated less than a minute ago

Instance ID i-0fb1e65047d86c419 (MyVm)	Public IPv4 address 35.74.244.171 open address	Private IPv4 addresses 10.0.1.78
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-1-78.ap-northeast-1.compute.internal	Private IP DNS name (IPv4 only) ip-10-0-1-78.ap-northeast-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 35.74.244.171 [Public IP]	VPC ID vpc-0a39e34261d4eaba3 (MyVpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0e45f1c450b8fb448 (mysubnet-1)	

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance details

Platform Amazon Linux (Inferred)	AMI ID ami-0329eac6c5240c99d	Monitoring disabled
Platform details Linux/UNIX	AMI name amzn2-ami-kernel-5.10-hvm-2.0.20230221.0-x86_64-gp2	Termination protection Disabled
Stop protection Disabled	Launch time Sun Mar 05 2023 12:36:55 GMT+0530 (India Standard Time) (4 minutes)	AMI location amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230221.0-x86_64-gp2
Instance auto-recovery Default	Lifecycle -	Stop-hibernate behavior -

- **Creating IAM role that will allow the EC2 instance to communicate with Cloudwatch:**

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

IAM > Roles > Create role

Step 1: Select trusted entity

Select trusted entity [Info](#)

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

- ☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **Lambda**
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:
Choose a service to view use case

[Cancel](#) [Next](#)

- **Selecting the CloudWatchAgentServerPolicy policy**

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

IAM > Roles > Create role

Step 2: Add permissions

Add permissions [Info](#)

Permissions policies (Selected 1/817) [Info](#)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 1 match

CloudWatchAgentServerPolicy X [Clear filters](#)

<input checked="" type="checkbox"/>	Policy name ?	Type	Description
<input checked="" type="checkbox"/>	CloudWatchAgentS...	AWS m...	Permissions required to use AmazonCloudWatchAgent on servers

► **Set permissions boundary - optional** [Info](#)
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

[Cancel](#) [Previous](#) [Next](#)

- **Attach the IAM Role to the EC2 instance**

EC2 > Instances > i-0fb1e65047d86c419 > Modify IAM role

Modify IAM role [Info](#)
Attach an IAM role to your instance.

Instance ID
i-0fb1e65047d86c419 (MyVm)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

CloudwatchLog [Create new IAM role](#)

[Cancel](#) [Update IAM role](#)

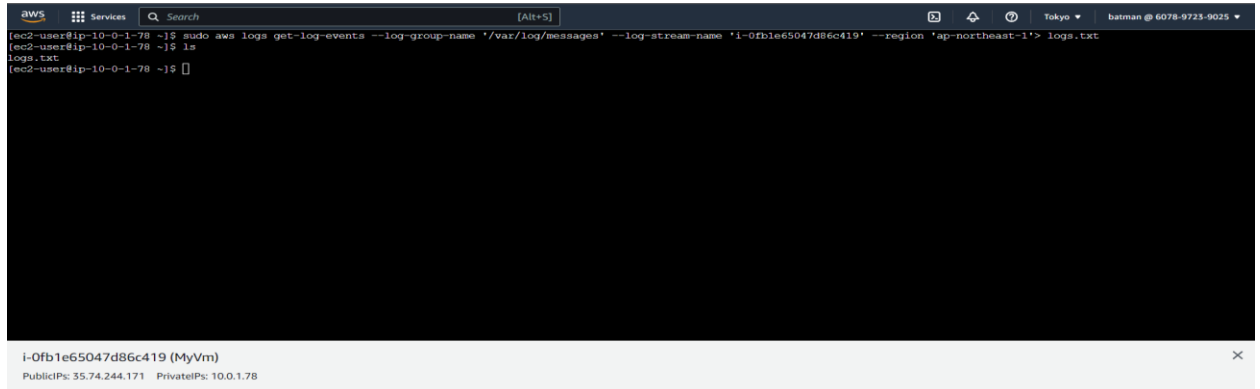
- `Vi /etc/awslogs/awscli.conf`

i-0fb1e65047d86c419 (MyVm)
PublicIPs: 35.74.244.171 PrivateIPs: 10.0.1.78

- after the agent has been running for a few moments**



- **Command to store the logs from cloudwatch into the Logs.txt file**
 - `sudo aws logs get-log-events --log-group-name '/var/log/messages' --log-stream-name 'i-0fb1e65047d86c419' --region 'ap-northeast-1' > logs.txt`



```
aws
Services
Search
[Alt+S]
Tokyo
batman @ 6078-9723-9025
(ec2-user@ip-10-0-1-78 ~)$ sudo aws logs get-log-events --log-group-name '/var/log/messages' --log-stream-name 'i-0fb1e65047d86c419' --region 'ap-northeast-1' > logs.txt
(ec2-user@ip-10-0-1-78 ~)$ ls
logs.txt
(ec2-user@ip-10-0-1-78 ~)$
```

i-0fb1e65047d86c419 (MyVm)
PublicIPs: 35.74.244.171 PrivateIPs: 10.0.1.78

Note:

While getting error of access denied to get the logs from cloudwatch. So modified the IAM role and added "logs:getLogEvents" in the policys so the role can get the details