

Special Offer | Flat 15% OFF SITEWIDE | Use Coupon - WHIZSITE15



[Home](#) > [My Courses](#) > [AWS Certified Solutions Architect Associate](#) > [CSAA Practice Test 6](#) > **Report**

Search Courses

🔍

CSAA Practice Test 6

Completed on 21-October-2020



**Attempt**  
03



**Marks Obtained**  
0 / 65



**Your score**  
0.0%



**Time Taken**  
N/A



**Result**  
Failed

Domains wise Quiz Performance Report

 Join us on **Slack community**

|                   |                                      |
|-------------------|--------------------------------------|
| No                | 1                                    |
| Domain            | Design High-Performing Architectures |
| Total Question    | 34                                   |
| Correct           | 0                                    |
| Incorrect         | 0                                    |
| Unattempted       | 34                                   |
| Marked for review | 0                                    |

|                   |  |
|-------------------|--|
| No                | 2  |
| Domain            | Design Resilient Architectures               |
| Total Question    | 10   |
| Correct           | 0  |
| Incorrect         | 0  |
| Unattempted       | 10   |
| Marked for review | 0  |
| No                | 3  |
| Domain            | Design Secure Applications and Architectures |
| Total Question    | 15   |
| Correct           | 0  |
| Incorrect         | 0  |
| Unattempted       | 15   |
| Marked for review | 0  |
| No                | 4  |
| Domain            | Design Cost-Optimized Architectures          |
| Total Question    | 6  |
| Correct           | 0  |
| Incorrect         | 0  |
| Unattempted       | 6  |
| Marked for review | 0  |
| Total             | Total  |
| All Domain        | All Domain                                   |
| Total Question    | 65   |
| Correct           | 0  |
| Incorrect         | 0  |
| Unattempted       | 65   |
| Marked for review | 0  |

Review the Answers

Sorting by

All

Question 1

Unattempted

Domain :Design High-Performing Architectures

Your company is planning on hosting a set of EC2 Instances in AWS. The Instances would be configured in a way that one will be used as a web tier and the other as a database (EC2 Hosted). The web tier should be exposed to the Internet in the Public Subnet and Database is in Private Subnet in the same VPC with the default configuration. What configuration needs to be done in order to let Web Server communicate with Database Server?

- A. Change the main route tables to have the desired routing between the subnets
- B. Ensure that the Security Groups have the required rules defined to allow traffic
- C. Ensure that all instances have a public IP for communication
- D. Ensure that all subnets are defined as public subnets

---

**Explanation:**

Answer – B

The AWS Documentation mentions the following

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC

**Main route table**

The first entry is the default entry for local routing in the VPC; this entry enables the instances in the VPC to communicate with each other.

| Destination |
|-------------|
| Target      |
| 10.0.0.0/16 |
| local       |

Option A is invalid since the main route table will have the required rules to route traffic between subnets in a VPC (By default). No change is required there.

Refer below URL for more details,

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario2.html#VPC\\_Scenario2\\_Routing](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html#VPC_Scenario2_Routing)

Option C is invalid since the instances would communicate with each other on the private IP

The primary reason to use the Private IP of an EC2 instance is to route the traffic internally within your VPC.

If you use the private IP to communicate, traffic will stay within the VPC, it will not be routed out, the routing table will route it internally

Option D is invalid since the database should be in the private subnet and not the public subnet

**This question asks for communication between subnets.**

For more information on Security Groups, please visit the below URL:

[http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_SecurityGroups.htm](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.htm)

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 2

Unattempted

Domain :Design Resilient Architectures

You work for a company that has a set of EC2 Instances. There is an internal requirement to create another instance in another availability zone. One of the EBS volumes from the current instance needs to be moved from one of the older instances to the new instance. How can you achieve this?

- A. Detach the volume and attach to an EC2 instance in another AZ.
- B. Create a new volume in the other AZ and specify the current volume as the source.
- C. Create a snapshot of the volume and then create a volume from the snapshot in the other AZ
- D. Create a new volume in the AZ and do a disk copy of contents from one volume to another.

---

**Explanation:**

Answer – C

In order for a volume to be available in another availability zone, you need to first create a snapshot from the volume. Then in the snapshot from creating a volume from the snapshot, you can then specify the new availability zone accordingly.

The **EBS Volumes attached to the EC2 Instance will always have to remain in the same availability zone as the EC2 Instance**. A possible reason for this could be because of the fact that EBS Volumes are present outside of the host machine and instances have to be connected over the network, if the EBS Volumes are present outside the Availability Zone there can be potential latency issues and subsequent performance degradation.

What one can do in such scenario is, get the Snapshot of the EBS Volume (Snapshot sequentially captures the state of your EBS Volume, you can **create an EBS Volume from this snapshot in your desired Availability Zone** and attach it to your new Instance

Later you can detach the volume from the older instance and delete then.

## Create Volume

Snapshot ID ⓘ

snap-0da3eeba923b18240 (Demo)

Volume Type ⓘ

General Purpose SSD (GP2) ▼

Size (GiB) ⓘ

8

(Min: 8 GiB, Max: 16384 GiB)

IOPS ⓘ

100 / 3000

(Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Throughput (MB/s) ⓘ

Not Applicable

Availability Zone ⓘ

ap-southeast-1a ▼

Encryption ⓘ

Not Encrypted

Cancel

Create

Option A is invalid because the Instance and Volume have to be in the same AZ in order for it to be attached to the instance because we have to specify AZ while creating Volume

Option B is invalid because there is no way to specify a volume as a source

Option D is invalid because the Diskcopy would just be a tedious process

For more information on snapshots, please visit the below URL

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ebs-detaching-volume.html>

## Try now labs related to this question

### Creating AMI From EC2 Instance

This lab walks you through the steps to create AMI from Amazon EC2 Instance. You will practice using Amazon Machine Images to launch Amazon EC2 Instance and Create AMI of that EC2 Instance.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

Question 3

Unattempted

Domain :Design Secure Applications and Architectures

Your team has developed an application and now needs to deploy that application onto an EC2 Instance. This application interacts with a DynamoDB table. Which of the following is the correct and MOST SECURE way to ensure that the application interacts with the DynamoDB table

- A. Create a role which has the necessary permissions and can be assumed by the EC2 instance
- B. Use the API credentials from an EC2 instance. Ensure the environment variables are updated with the API access keys.
- C. Use the API credentials from a bastion host. Make the application on the EC2 Instance send requests via the bastion host.
- D. Use the API credentials from a NAT Instance. Make the application on the EC2 Instance send requests via the NAT Instance

Explanation:

Answer – A

IAM roles are designed in such a way so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

Options B, C, and D are invalid because it is not secure to use API credentials from any EC2 instance. The API credentials can be tampered with and hence is not the ideal secure way to make API calls.

For more details on AWS Credentials, please refer below URL

<https://aws.amazon.com/blogs/security/what-to-do-if-you-inadvertently-expose-an-aws-access-key/>

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_access-keys.html#Using\\_CreateAccessKey\\_API](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey_API)

For more information on IAM roles for EC2, please refer below URL:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

---

### Try now labs related to this question

#### Introduction to AWS Identity Access Management(IAM)

This lab walks you through the steps on how to create IAM Users, IAM Groups and adding IAM User to the IAM Group in AWS IAM service

💎 Credit Needed 0 ⌚ Time 0 : 20

Try Now

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 4

Unattempted

Domain :Design Secure Applications and Architectures

You are using Amazon RDS as a relational database for your web application in AWS. All your data stored in Amazon RDS is encrypted using AWS KMS. Encrypting this data is handled by a separate team of 4 users (User A, B, C, & D) in Security Team. They have created 2 CMK's for encryption of data.

During annual Audit, there were concerns raised by Auditors for access to these CMK's for each user. Security Team has following IAM Policy & Key Policy set for AWS KMS.

- CMK1 is created by AWS KMS API & has a default Key policy.
- CMK2 is default key policy created by AWS Management console & allows User D.
- User C has IAM Policy denying all action for CMK1 while allowing for CMK2.
- User A & User B has IAM Policy allowing access to CMK1 while denying access to CMK2.
- User D has IAM policy allowing full access to AWS KMS.

Which of the following is correct statement for access each user has for AWS KMS CMK?

- A. User A & B can use the only CMK1, user C cannot use CMK1, while user D can use both CMK1 & CMK2.
- B. User A & B can use CMK1& CMK2, user C can use only CMK2, while user D can use both CMK1 & CMK2.
- C. User A & B can use CMK1, user C can use CMK1 & CMK2, while user D can use both CMK1 & CMK2.
- D. User A & B can use only CMK1, user C can use only CMK2, while user D cannot use both CMK1 & CMK2.

---

#### Explanation:

#### Correct Answer – A

Access to AWS KMS CMK is a combination of both Key policy & IAM policy. IAM Policy should grant access to a user for AWS KMS. While Key Policy is used to control access to CMK in AWS KMS.

Option B is incorrect as CMK2 key policy do not grant access to User C. Also, User A & B do not have IAM policy to access CMK2.

Option C is incorrect as CMK2 key policy do not grant access to User C. Also, it does not have IAM policy to access CMK1.

Option D is incorrect as User D has IAM policy & Key Policy to use both CMK1 & CMK2.

For more information on determining access to AWS KMS CMK, refer to following URL,

<https://docs.aws.amazon.com/kms/latest/developerguide/determining-access.html>

---

Ask our Experts

Rate this Question? 😊 😞



## Question 5

Unattempted

## Domain :Design High-Performing Architectures

Your company is building container-based applications. Currently, they use Kubernetes for their on-premises docker based orchestration. They want to move to AWS and preferably not have to manage the infrastructure for the underlying orchestration service. Which of the following could be used for this purpose?

- A. AWS DynamoDB
- B. AWS ECS with EC2 launch type
- C. AWS EC2 with Kubernetes installed
- D. AWS Elastic beanstalk

---

**Explanation:**

Answer – D

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

Option A is incorrect since this is a fully managed NoSQL database

Option B is incorrect because you have to manage infrastructure.

Option C is incorrect since this would add maintenance overhead for the company and the question mentions that the company does not want to manage the infrastructure

**Elastic Beanstalk vs ECS** really comes down to control. Do you want to control your scaling and capacity or do you want to have that more abstracted and instead focus primarily on your app? ECS will give you control, as you have to specify the size and number of nodes in the cluster and whether or not auto-scaling should be used. With Elastic Beanstalk, you simply provide a Dockerfile and Elastic Beanstalk takes care of scaling your provisioning of number and size of nodes, you basically can forget about the infrastructure with the Elastic Beanstalk route.

For more information on Elastic Beanstalk, please visit the below URL:

[http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create\\_deploy\\_docker.html](http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html)

With ECS you'll have to build the infrastructure first before you can start deploying the Dockerfile.

For more information on AWS ECS service, please visit the below URL:

<https://aws.amazon.com/ecs/>

<https://aws.amazon.com/blogs/aws/amazon-elastic-container-service-for-kubernetes/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 6

Unattempted

Domain :Design High-Performing Architectures

Your company is looking at decreasing the amount of time it takes to build servers that are deployed as EC2 Instances. These Instances always have the same type of software installed as per the security standards. As an architect what would you recommend in decreasing the server build time?

- A. Look at creating snapshots of EBS Volumes
- B. Create the same master copy of the EBS volume
- C. Create a custom AMI
- D. Create a base profile

---

**Explanation:**

Answer – C

The AWS Documentation mentions the following

An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You must specify a source AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration. You can use different AMIs to launch instances when you need instances with different configurations.

You can launch an instance from an existing AMI, customize the instance, and then save this updated configuration as a custom AMI. Instances launched from this new custom AMI include the customizations that you made when you created the AMI.

Options A and B are incorrect since these cannot be used to create a master copy of the instance

Option D is incorrect because creating a profile will not assist

For more information on AMI's, please visit the below URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

---

## Try now labs related to this question

### Creating AMI From EC2 Instance

This lab walks you through the steps to create AMI from Amazon EC2 Instance. You will practice using Amazon Machine Images to launch Amazon EC2 Instance and Create AMI of that EC2 Instance.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 7

Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Administrator for a global IT company. The Software team has developed a new application for Project delivery deployed on AWS. Changes in the application are done on a quarterly basis and will be deployed on a new redundant infrastructure. The company would like to automate this process of development changes and provisioning of resources. For deploying new features, AWS CodePipeline will be used for an automated release cycle. What would you recommend as a source stage and deploy stage integration along with AWS CodePipeline?

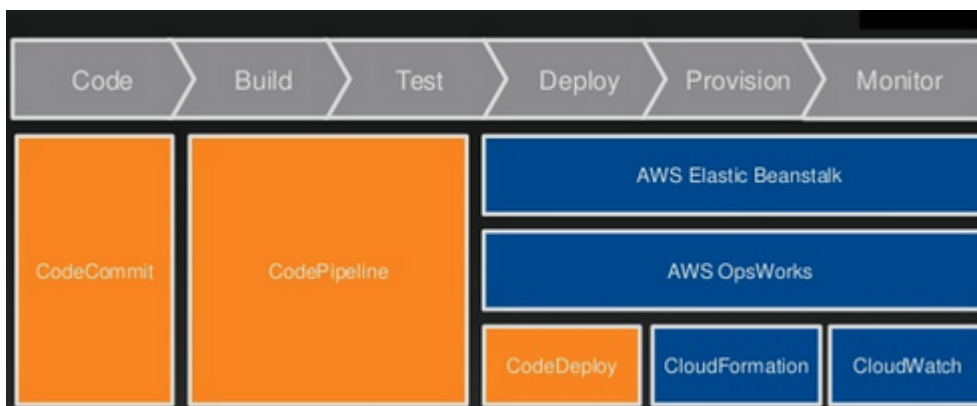
- A. Use CodePipeline with source stage as CodeCommit and deploy stage using AWS CodeDeploy.

- B. Use CodePipeline with source stage as CodeCommit and deploy stage using AWS Elastic Beanstalk.
- C. Use CodePipeline with source stage as S3 bucket having versioning enable and deploy stage using AWS Elastic Beanstalk.
- D. Use CodePipeline with source stage as S3 bucket having versioning enable and deploy stage using AWS Code Deploy.

---

**Explanation:****Correct Answer – B**

AWS CodeCommit can be used as a source stage integration with AWS CodePipeline. Also, new infrastructure needs to be built for this new application deployment, AWS Elastic Beanstalk can be used to build & manage redundant resources.



Option A is incorrect. There is no existing infrastructure. As a new resource needs to be provisioned, AWS Code Deploy is not a correct option.

Options C and D are incorrect as using S3 as a source is not recommended for Software Development because CodeCommit is optimized for team software development. It manages batches of changes across multiple files, which can occur in parallel with changes made by other developers. Amazon S3 versioning supports the recovery of past versions of files, but it's not focused on collaborative file tracking features that software development teams need. Refer below URL for details

<https://docs.aws.amazon.com/codecommit/latest/userguide/welcome.html#welcome-arc-vs-s3>

For more information on AWS CodePipeline Integration type, refer to the following URL:

<https://docs.aws.amazon.com/codepipeline/latest/userguide/integrations-action-type.html>

---

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ✓

Question 8

Unattempted

Domain :Design High-Performing Architectures

You are designing the following application in AWS. Users will use the application to upload videos and images. The files will then be picked up by a worker process for further processing. Which of the below services should be used in the design of the application. Choose 2 answers from the options given below

- A. AWS Simple storage service for storing the videos and images
- B. AWS Glacier for storing the videos and images
- C. AWS SNS for distributed processing of messages by the worker process
- D. AWS SQS for distributed processing of messages by the worker process

**Explanation:**

Answer - A and D

The AWS Documentation mentions the following

Amazon Simple Storage Service is storage for the Internet. It is designed to make web-scale computing easier for developers.

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

Based on S3 Bucket events, you can trigger the SQS Queue.

You can go in Bucket properties and select the event and choose SQS Queue

### Transfer acceleration

Enable fast, easy and secure transfers of files to and from your bucket.

[Learn more](#)

☐ Suspended

### Events

[+ Add notification](#) [Delete](#) [Edit](#)

| Name  | Events | Filter | Type |
|---|--------|--------|------|
| New event   |        |        |      |
| <b>Name</b> ⓘ<br><input type="text" value="e.g. MyEmailEventForPut"/>   |        |        |      |
| <b>Events</b> ⓘ <div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"> <input type="checkbox"/> PUT<br/> <input type="checkbox"/> POST<br/> <input type="checkbox"/> COPY<br/> <input type="checkbox"/> Multipart upload completed<br/> <input type="checkbox"/> All object create events<br/> <input type="checkbox"/> Object in RRS lost<br/> <input type="checkbox"/> Permanently deleted<br/> <input type="checkbox"/> Delete marker created           </div> <div style="width: 50%;"> <input type="checkbox"/> All object delete events<br/> <input type="checkbox"/> Restore initiated<br/> <input type="checkbox"/> Restore completed<br/> <input type="checkbox"/> Replication time missed threshold<br/> <input type="checkbox"/> Replication time completed after threshold<br/> <input type="checkbox"/> Replication time not tracked<br/> <input type="checkbox"/> Replication failed           </div> </div> |        |        |      |
| <b>Prefix</b> ⓘ<br><input type="text" value="e.g. images/"/>  |        |        |      |
| <b>Suffix</b> ⓘ<br><input type="text" value="e.g. .jpg"/>   |        |        |      |
| <b>Send to</b> ⓘ<br><div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px;">SQS Queue</div> <div style="background-color: #0070c0; color: white; padding: 2px;">SNS Topic</div> <div style="background-color: #0070c0; color: white; padding: 2px;">SQS Queue</div> <div style="background-color: #0070c0; color: white; padding: 2px;">Lambda Function</div> </div>  |        |        |      |
| <input type="radio"/> 0 Active notifications <div style="float: right;"> <a href="#">Cancel</a> <a href="#">Save</a> </div>   |        |        |      |

### Requester pays

The requester (instead of the bucket owner) will pay for requests and data transfer.

[Learn more](#)

☐ Disabled

Option B is incorrect since this is used for archive storage

Option C is incorrect since this is used as a notification service

For more information on S3, please visit the below URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html>

For more information on SQS, please visit the below URL:

<https://aws.amazon.com/sqs/>

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ✓

Question 9

Unattempted

Domain :Design High-Performing Architectures

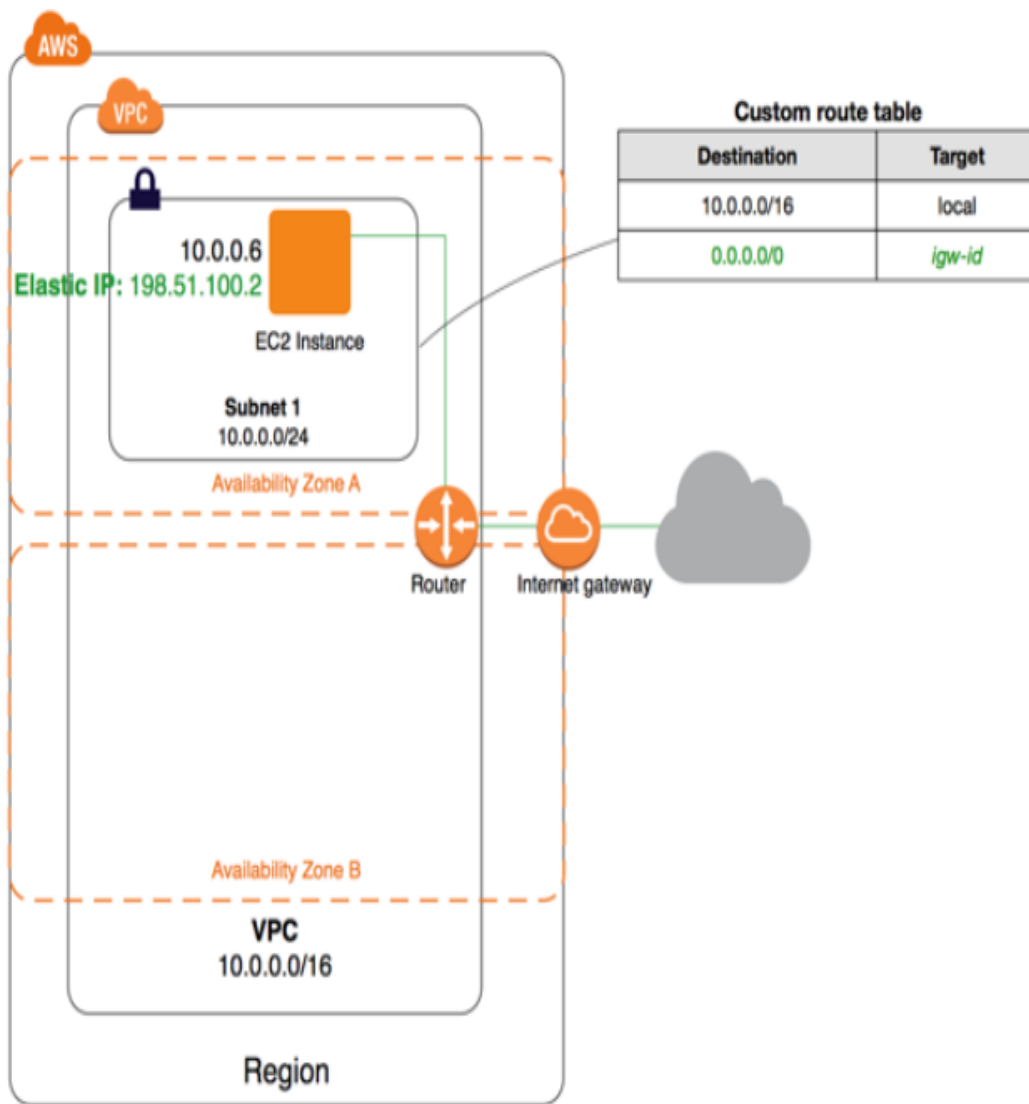
Your development team has created a web application in a subnet that needs to be tested. You need to advise the IT admin team on how they should configure the VPC to ensure the application can be accessed from the Internet. Which of the following components would be part of the design. Choose 3 answers from the options given below

- A. An Internet gateway attached to the VPC.
- B. A NAT gateway attached to the VPC.
- C. Custom Route table entry added for the Internet gateway
- D. All instances launched with a public IP

**Explanation:**

Answer - A, C and D

The configuration for this scenario includes a virtual private cloud (VPC) with a single public subnet, and an internet gateway to enable communication over the internet



An internet gateway. This connects the VPC to the internet and to other AWS services.

A custom route table associated with the subnet. The route table entries enable instances in the subnet to use IPv4 to communicate with other instances in the VPC, and to communicate directly over the internet. A subnet that's associated with a route table that has a route to an internet gateway is known as a public subnet.

Instances receive a Public IP address so that it is reachable from outside the VPC. This IP address might change if the instance stops and starts. Alternatively, you can use an Elastic IP Address that remains static.

Only use a Public IP/Elastic IP address when communicating with the instance from outside the VPC.

Option B is incorrect since this should be used for communication of instances in the private subnet to the Internet

For more information on public subnets and the VPC, please visit the below URL:





[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario1.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

## Try now labs related to this question

### Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.
2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

 Credit Needed 10     Time 0 : 30

Try Now

Ask our Experts

Rate this Question?  

View Queries

open 

Question 10

Unattempted

Domain :Design Secure Applications and Architectures

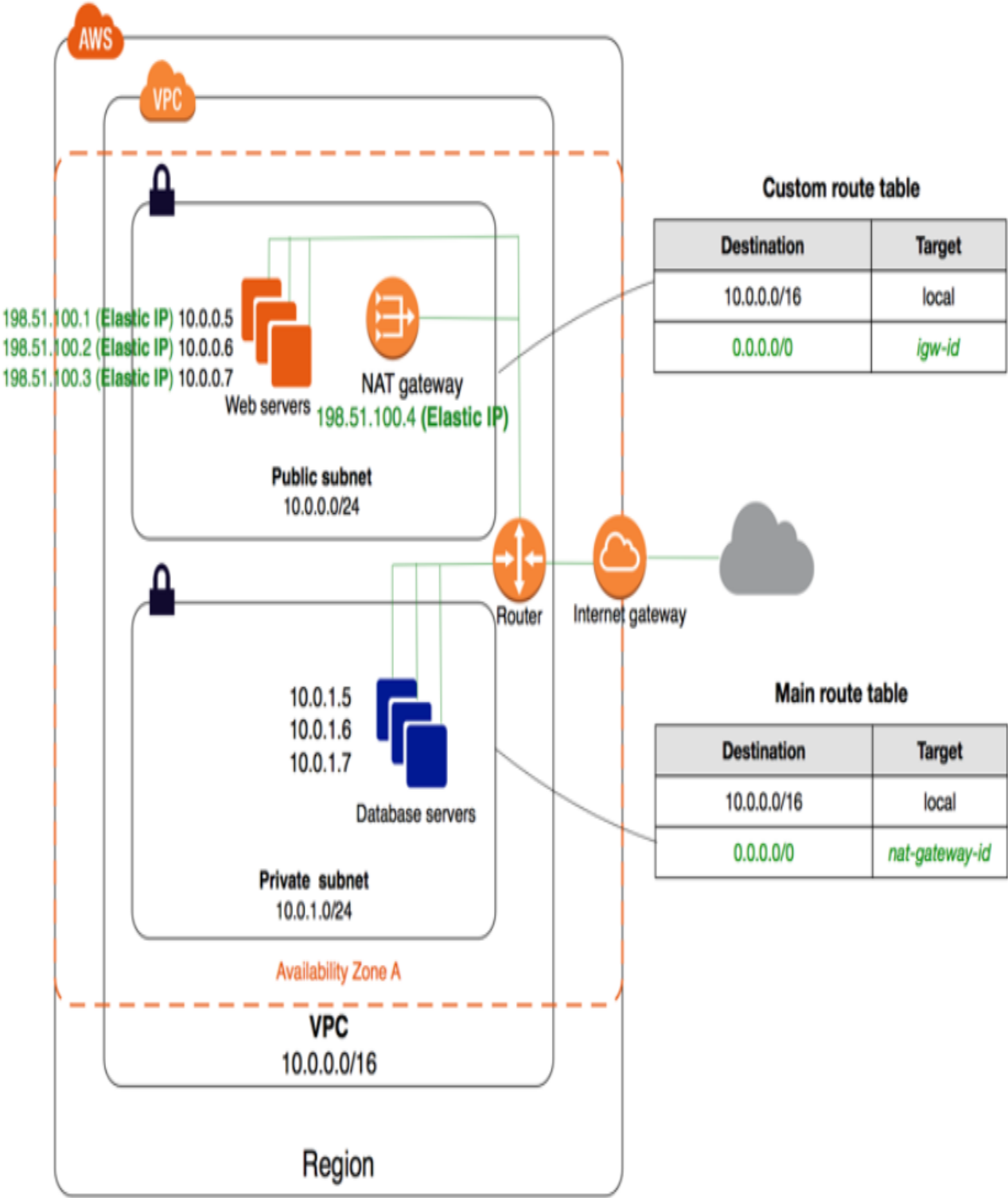
Your company is planning on deploying an application which will consist of a web and database tier. The database tier should not be accessible from the Internet. How would you design the networking part of the application? Choose 2 answers from the options below

- A. A public subnet for the web tier
- B. A private subnet for the web tier
- C. A public subnet for the database tier
- D. A private subnet for the database tier

### Explanation:

Answer - A and D

The below diagram from the AWS Documentation shows the design of a web and database tier



Option B is incorrect since users will not be able to access the web application if it placed in a private subnet

Option C is incorrect since the question mentions that the database should not be accessible from the internet

For more information on private and public subnets and the VPC, please visit the below URL:



[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

---

### Try now labs related to this question

#### Build Amazon VPC with Public and Private Subnets from Scratch

1. Learn how to build Public and Private subnets from scratch.
2. VPC wizard will not be used. So every component required to build public and private subnets will be created and configured manually.
3. This will give an in-depth understanding of internal components of VPC and subnets.

 Credit Needed 10     Time 0 : 30

Try Now

Ask our Experts

Rate this Question?  

---

View Queries

open 

Question 11

Unattempted

Domain :Design Resilient Architectures

You are creating a number of EBS Volumes for the EC2 Instances hosted in your company's AWS account. The company has asked you to ensure that the EBS volumes are available even in the case of an entire region facing an outage due to a natural disaster. How would you accomplish this? Choose 2 answers from the options given below

- A. **Configure Amazon Storage Gateway with EBS volumes as the data source and store the backups on premise through the storage gateway**
- B. **Create snapshots of the EBS Volumes.**
- C. **Ensure the snapshots are made available in another availability zone**
- D. **Ensure the snapshots are made available in another region**

---

**Explanation:**

Answer - B and D

The AWS Documentation mentions the following

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.

Option A is incorrect since you have to make use of EBS snapshots

Option C is incorrect since the snapshots need to be made available in another region for such a huge disaster. It may be rare for the whole AWS region to go down, but it could cause massive permanent damage if we don't plan for it.

For more information on EBS snapshots, please visit the below URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

**View Queries**

open ▾

Question 12

Unattempted

## Domain :Design High-Performing Architectures

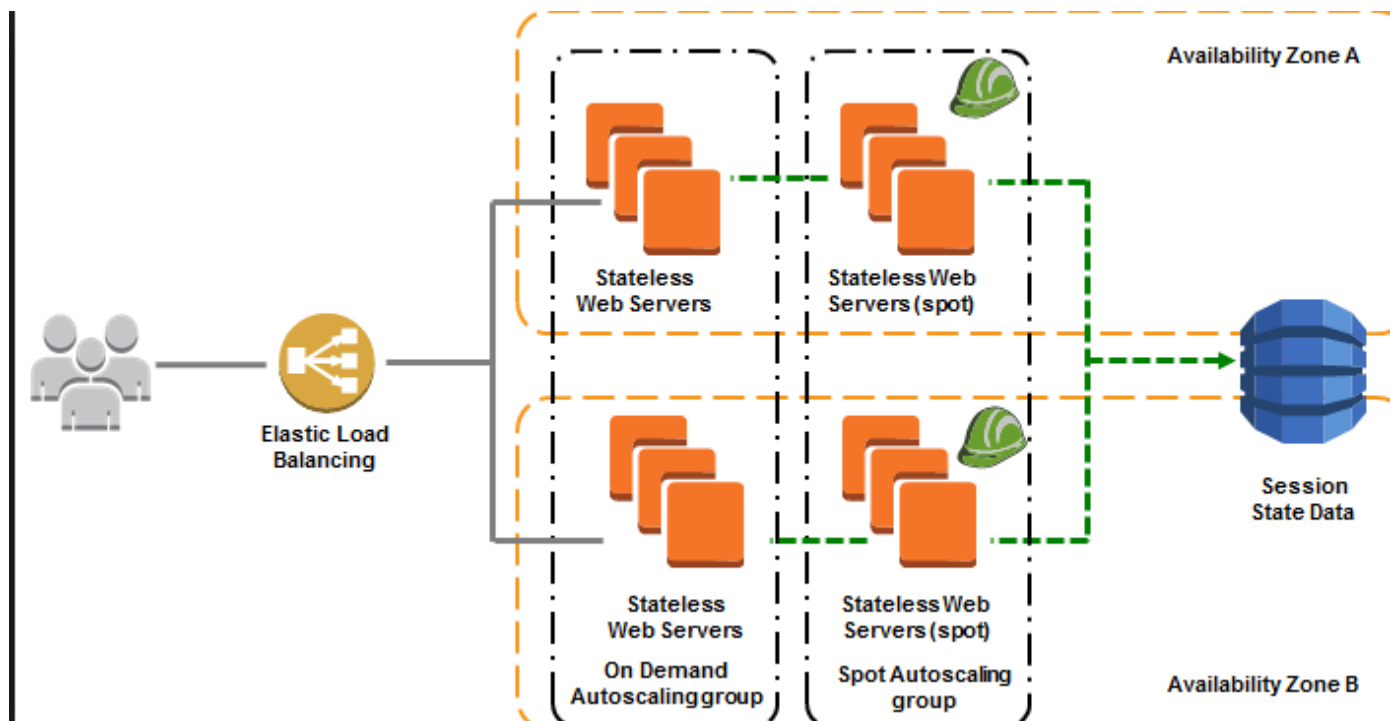
You are planning on hosting a static website on EC2 Instances. You need to ensure that the environment is highly available and scalable to meet demand. Which of the below aspects can be used to create a highly available environment. Choose 3 answers from the options given below.

- A. Auto Scaling group
- B. Elastic Load Balancer
- C. SQS queue
- D. Multiple Availability Zones

**Explanation:**

Answer - A, B and D

The diagram below shows an example of a highly available architecture for hosting EC2 Instances



Here you have the

ELB is placed in front of the users which helps in directing the traffic to the EC2 Instances.

The EC2 Instances which are placed as part of an AutoScaling Group

Then you have multiple subnets which are mapped to multiple availability zones

The solution is to create several instances across several availability zones and to use an elastic load balancer to distribute the traffic and Auto Scaling group to scale the instances. This way, even if an instance fails, you already have other ones available. AWS recommends this solution as they have an SLA of 99.95% for their instance in an AZ. By putting in several AZs you can have 100% availability

For a static web site, the SQS is not required to build such an environment. If you have a system such as an order processing system, which has that sort of queuing of requests, then that could be a candidate for using SQS Queues.

For more information on high availability, please visit the below URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html#scale-and-load-balance-prerequisites>

---

## Try now labs related to this question

### Introduction to Amazon Auto Scaling

AWS Auto Scaling will automatically scale resources as needed to align to your selected scaling strategy. This lab walks you through to use Auto Scaling to automatically launch or terminate EC2's instances based on user defined policies, schedules and health checks.

💎 Credit Needed 10 ⌚ Time 0 : 55

Try Now

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 13

Unattempted

Domain :Design High-Performing Architectures

A global media firm is using AWS CodePipeline as an automation service for releasing new features to customers. All the codes are uploaded in the Amazon S3 bucket. Changes in files stored in the S3 bucket should trigger AWS CodePipeline that will further initiate AWS Elastic Beanstalk for deploying additional resources. What is the additional requirement that should be configured to trigger CodePipeline in a faster way?

- A. Enable periodic checks and create a Webhook which triggers pipeline once S3 bucket is updated.
- B. Disable periodic checks, create an Amazon CloudWatch Events rule & AWS CloudTrail trail.
- C. Enable periodic checks, create an Amazon CloudWatch Events rule & AWS CloudTrail trail.
- D. Disable periodic checks and create a Webhook which triggers pipeline once S3 bucket is updated.

---

**Explanation:****Correct Answer – B**

To automatically trigger pipeline with changes in the source S3 bucket, Amazon CloudWatch Events rule & AWS CloudTrail trail must be applied. When there is a change in the S3 bucket, events are filtered using AWS CloudTrail & then Amazon CloudWatch events are used to trigger the start of the pipeline. This default method is faster & periodic checks should be disabled to have events-based triggering of CodePipeline.

You can use the following tools to monitor your CodePipeline pipelines and their resources:

**Amazon CloudWatch Events** — Use Amazon CloudWatch Events to detect and react to pipeline execution state changes (for example, send an Amazon SNS notification or invoke a Lambda function).

**AWS CloudTrail** — Use CloudTrail to capture API calls made by or on behalf of CodePipeline in your AWS account and deliver the log files to an Amazon S3 bucket. You can choose to have CloudWatch publish Amazon SNS notifications when new log files are delivered so you can take quick action.

**Console and CLI** — you can use the CodePipeline console and CLI to view details about the status of a pipeline or a particular pipeline execution.

Option A is incorrect as Webhooks are used to trigger pipeline when the source is GitHub repository. Also, the periodic check will be a slower process to trigger CodePipeline.

Option C is incorrect as Periodic checks are not a faster way to trigger CodePipeline.

Option D is incorrect as Webhooks are used to trigger pipeline when the source is GitHub repository.

For more information on Automatically Triggering Pipeline, refer to the following URL:

<https://docs.aws.amazon.com/codepipeline/latest/userguide/pipelines-about-starting.html>

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ✓

Question 14

Unattempted

Domain :Design Resilient Architectures

You have a requirement to host a web based application. You need to enable high availability for the application, so you create an Elastic Load Balancer and place the EC2 Instances behind the Elastic Load Balancer. You need to ensure that users only access the application via the DNS name of the load balancer. How would you design the network part of the application? Choose 2 answers from the options below

- A. Create 2 public subnets for the Elastic Load Balancer
- B. Create 2 private subnets for the Elastic Load Balancer
- C. Create 2 public subnets for the EC2 Instances
- D. Create 2 private subnets for the EC2 Instances

**Explanation:**

Answer - A and D

The AWS Documentation mentions the following

**Use Case: A load balancer, two public subnets, two private subnets, two NAT Gateways,**

The NAT Gateway goes into both public subnets (Public-Subnet-A, Public-Subnet-B)

The EC2 instances are launched in private subnets across two AZs (Private-Subnet-A, Private-Subnet-B)

The Route Table Private-Subnet-A points to the NAT Gateway in Public-Subnet-A

The Route Table Private-Subnet-B points to the NAT Gateway in Public-Subnet-B

If one of the AZs should fail, then the EC2 instances in the remaining private subnet will still be able to communicate with the Internet because they have their own NAT Gateway in that AZ.



Option B is incorrect since the ELB needs to be placed in the public subnet to allow access from the Internet

Option C is incorrect based on security issues. Private subnet gives us better security from the attacks.



For more information on an example to use the Load balancer, please visit the below URL:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

## Try now labs related to this question

### Introduction to AWS Elastic Load Balancing

This lab walks you through AWS Elastic Load Balancing. Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. In this lab, we will demonstrate elastic load balancing with 2 EC2 Instances.

 Credit Needed 10     Time 0 : 30

[Try Now](#)

[Ask our Experts](#)

Rate this Question?  

[View Queries](#)

[open](#) 

Question 15

Unattempted

Domain :Design High-Performing Architectures

You are working as an AWS Architect for a retail company using AWS EC2 instance for a web application. The company is using Provisioned IOPS SSD EBS volumes to store all product database. This is a critical database & you need to ensure appropriate backups are accomplished every 12 hours. Also, you need to ensure that storage space is optimally used for storing all these snapshots removing all older files. Which of the following can help to meet this requirement with the least management overhead?

- A. Manually create snapshots & delete old snapshots for EBS volumes as this is a critical data.
- B. Use Amazon CloudWatch events to initiate AWS Lambda which will create snapshot of EBS volumes along with deletion of old snapshots.

- C. Use Amazon Data Lifecycle Manager to schedule EBS snapshots and delete old snapshots as per retention policy.
- D. Use Third party tool to create snapshot of EBS volumes along with deletion of old snapshots.

---

**Explanation:****Correct Answer – C**

Amazon Data Lifecycle Manager can be used for creation, retention & deletion of EBS snapshots. It protects critical data by initiating backup of Amazon EBS volumes at selected intervals, along with storing & deletion of old snapshots to save storage space & cost.

Option A is incorrect as this will result in additional admin work & there can be a risk of losing critical data due to manual errors.

Option B is incorrect as for this we will need to do additional config changes in CloudWatch & AWS Lambda. Also, AWS Lambda would need a script to create snapshots which can be an overhead

Option D is incorrect as this will result in an additional cost to maintain a third-party software.

For more information on Automating Amazon EBS Snapshot Lifecycle, refer to the following URL,

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

**View Queries**

open ▼

**Question 16**

**Unattempted**

**Domain :Design High-Performing Architectures**

You work as an architect for a consulting company. The consulting company normally creates the same set of resources for their clients. They want some way of building templates, which can then be used to deploy the resources to the AWS accounts for the various clients. Also, your team needs to be ensured that they have control over the infrastructure. Which of the following service can help fulfill this requirement?

- A. AWS Elastic Beanstalk

- B. Custom AMI
- C. AWS Cloudformation
- D. EBS Snapshots

---

**Explanation:**

Answer – C

The AWS Documentation mentions the following

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.

Elastic Beanstalk is intended to make developers' lives easier. CloudFormation is intended to make systems engineers' lives easier.

Elastic Beanstalk is a PaaS layer on top of AWS's IaaS services which abstracts away the underlying EC2 instances, Elastic Load Balancers, Auto Scaling groups, etc. This makes it a lot easier for developers, who don't want to be dealing with all the systems stuff, to get their application quickly deployed on AWS. With Elastic Beanstalk, you don't need to understand how any of the underlying magic works.

CloudFormation, on the other hand, doesn't automatically do anything. It's simply a way to define all the resources needed for deployment in a huge JSON file.

Option A could be a valid choice but it has been clearly asked in question that the team needs to have control over the infrastructure.

Option B is invalid because Custom AMI will help to create an Image for EC2 Instances not for all the resources.

Option D is invalid because EBS Snapshot is a copy of your Volume used for EC2 Instance.

For more information on CloudFormation, please visit the below URL:

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html>

---

**Try now labs related to this question**

**Introduction to Amazon CloudFormation**

This lab walks you through to AWS CloudFormation features. In this lab, we will demonstrate the use AWS CloudFormation Stack in creating a simple LAMP Server.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Question 17

Unattempted

Domain :Design Secure Applications and Architectures

You work as an architect for a company. An application is going to be deployed on a set of EC2 instances in a private subnet of VPC. You need to ensure that IT administrators can securely administer the instances in the private subnet. How can you accomplish this?

- A. Create a NAT gateway, ensure SSH access is provided to the NAT gateway. Access the Instances via the NAT gateway.
- B. Create a NAT instance in a public subnet, ensure SSH access is provided to the NAT instance. Access the Instances via the NAT instance.
- C. Create a bastion host in the private subnet. Make IT admin staff use this as a jump server to the backend instances.
- D. Create a bastion host in the public subnet. Make IT admin staff use this as a jump server to the backend instances.

### Explanation:

Answer – D

The AWS Documentation mentions the following

A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet. Because of its exposure to potential attack, a bastion host must minimize the chances of penetration. For example, you can use a bastion host to mitigate the risk of allowing SSH connections from an external network to the Linux instances launched in a private subnet of your Amazon Virtual Private Cloud (VPC).

Options A and B are invalid because you would not route access via the NAT instance or the NAT gateway

Option C is incorrect since the bastion host needs to be in the public subnet

For more information on bastion hosts please visit the below URL:

<https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 18

Unattempted

Domain :Design Secure Applications and Architectures

You work as an architect for a company. An application is going to be deployed on a set of EC2 instances in a VPC. The Instances will be hosting a web application. You need to design the security group to ensure that users have the ability to connect from the Internet via HTTPS. Which of the following needs to be configured for the security group

- A. Allow Inbound access on port 443 for 0.0.0.0/0
- B. Allow Outbound access on port 443 for 0.0.0.0/0
- C. Allow Inbound access on port 80 for 0.0.0.0/0
- D. Allow Outbound access on port 80 for 0.0.0.0/0

---

**Explanation:**

Answer – A

The AWS Documentation mentions the following

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance.

Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

AWS Security groups are stateful which means you do not need to open the outbound for responses - open only inbound for requests. If you think your instances will be sending requests to certain IPs (for example: to upgrade/install a package), then you need to open the IP/port for that request. By default, it is open for all traffic.

Option B is incorrect since security groups are stateful, you don't need to define the rule for outbound traffic

Options C and D are incorrect since you need to only ensure access for HTTPS, hence you should not configure rules for port 80

For more information on security groups, please visit the below URL:



[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

---

## Try now labs related to this question

### Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.
2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

 Credit Needed 10     Time 0 : 30

Try Now

Ask our Experts

Rate this Question?  

View Queries

open 

Question 19

Unattempted

Domain :Design High-Performing Architectures

Your company runs an automobile reselling company that has a popular online store on AWS. The application sits behind an Auto Scaling group and requires new instances of the Auto Scaling group to identify their public and private IP addresses. Which of the following is the correct AWS option to identify the IP addresses?

- A. By using Ipconfig for windows or Ifconfig for Linux.
- B. By using a CloudTrail.
- C. Using a Curl or Get Command to get the latest meta-data from <http://169.254.169.254/latest/meta-data/>
- D. Using a Curl or Get Command to get the latest user-data from <http://169.254.169.254/latest/user-data/>

---

**Explanation:**

Answer – C

To get the private and public IP addresses, you can run the following commands on the running instance

<http://169.254.169.254/latest/meta-data/local-ipv4>

<http://169.254.169.254/latest/meta-data/public-ipv4>

Option A is partially correct but it is an overhead when you already have the service running in AWS.

Option B is incorrect because CloudTrail is used for tracking the API activities of a resource

Option D is incorrect because user-data cannot get the IP addresses

For more information on instance metadata, please refer to the below URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html>

---

**Try now labs related to this question****Introduction to Amazon Auto Scaling**

AWS Auto Scaling will automatically scale resources as needed to align to your selected scaling strategy. This lab walks you through to use Auto Scaling to automatically launch or terminate EC2's instances based on user defined policies, schedules and health checks.

💎 Credit Needed 10    ⌚ Time 0 : 55

[Try Now](#)

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ✓

Question 20

Unattempted

Domain :Design High-Performing Architectures

You have been designing a CloudFormation template that creates one elastic load balancer fronting two EC2 instances. Which section of the template should you edit so that the DNS of the load balancer is returned upon creation of the stack?

- A. Resources
- B. Parameters
- C. Outputs
- D. Mappings

**Explanation:**

Answer – C

The below example shows a simple CloudFormation template. It creates an EC2 instance based on the AMI - ami-d6f32ab5. When the instance is created, it will output the AZ in which it is created.

```
{  
  
  "Resources": {  
  
    "MyEC2Instance": {  
  
      "Type": "AWS::EC2::Instance",  
  
      "Properties": {  
  
        "ImageId": "ami-d6f32ab5"  
  
      }  
    }  
  }  
}
```



```
}  
  
},  
  
"Outputs": {  
  
  "Availability": {  
  
    "Description": "The Instance ID",  
  
    "Value":  
  
    { "Fn::GetAtt" : [ "MyEC2Instance", "AvailabilityZone" ] }  
  
  }  
  
}  
  
}
```

Option A is incorrect because this is used to define the main resources in the template

Option B is incorrect because this is used to define parameters which can taken in during template deployment

Option D is incorrect because this used to map key value pairs in a template

To understand more on CloudFormation, please visit the url

<https://aws.amazon.com/cloudformation/>



<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-getatt.html>

---

## Try now labs related to this question

### Introduction to Amazon CloudFormation

This lab walks you through to AWS CloudFormation features. In this lab, we will demonstrate the use AWS CloudFormation Stack in creating a simple LAMP Server.

 Credit Needed 10     Time 0 : 30

[Try Now](#)

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ✓

Question 21

Unattempted

Domain :Design Secure Applications and Architectures

A company has a set of VPC's defined in AWS. They need to connect this to their on-premises network. They need to ensure that all data is encrypted in transit. Which of the following would you use to connect the VPC's to the on-premises networks?

- A. VPC Peering
- B. VPN connections
- C. AWS Direct Connect
- D. Placement Groups

**Explanation:**

Answer – B

The AWS Documentation mentions the following

By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by attaching a virtual private gateway to the VPC, creating a custom route table, updating your security group rules, and creating an AWS managed VPN connection.

VPN connection encrypts the traffic whereas Direct Connect does not encrypt your traffic that is in transit. To encrypt the data in transit that traverses AWS Direct Connect, you must use the transit encryption options for that service.

Option A is incorrect because this is used to connect multiple VPC's together.

Option C is incorrect because this does not encrypt traffic in connections between AWS VPC's and the On-premises network

Option D is incorrect because this is used for low latency access between EC2 Instances

For more information on AWS VPN connections and Direct Connect, please visit the below URL

[https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html#concepts](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html#concepts)

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-transit.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 22

Unattempted

Domain :Design High-Performing Architectures

A company wants to host a selection of MongoDB instances. They are expecting a high load and want to achieve high performance. As an architect, you need to ensure that the right storage is used to host the MongoDB database. Which of the following would you incorporate as the underlying storage layer?

- A. Provisioned IOPS
- B. General Purpose SSD
- C. Throughput Optimized HDD
- D. Cold HDD

---

**Explanation:**

Answer – A

The below snapshot from the AWS Documentation shows the different volume types and why Provisioned IOPS is the most ideal for this requirement

Also, Provisioned IOPS is recommended for NoSQL and Relational Databases.

## Solid State Drives (SSD)

## Hard Disk Drives (HDD)

| Volume Type       | EBS Provisioned IOPS SSD (io1)  | EBS General Purpose SSD (gp2)*   | Throughput Optimized HDD (st1)   | Cold HDD (sc1)   |
|-------------------|---|--|--|--|
| Short Description | Highest performance SSD volume designed for latency-sensitive transactional workloads | General Purpose SSD volume that balances price performance for a wide variety of transactional workloads | Low cost HDD volume designed for frequently accessed, throughput intensive workloads | Lowest cost HDD volume designed for less frequently accessed workloads |
| Use Cases         | I/O-intensive NoSQL and relational databases  | Boot volumes, low-latency interactive apps, dev & test   | Big data, data warehouses, log processing  | Colder data requiring fewer scans per day                              |

Because of what is mentioned in the documentation as the ideal storage type, the other options are invalid.

For more information on the different EBS volume types, please visit the below URL

<https://aws.amazon.com/ebs/details/>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

Question 23

Unattempted

Domain :Design Secure Applications and Architectures

A customer needs corporate IT governance and cost oversight of all AWS resources consumed by its divisions. Each division has its own AWS account and there is a need to ensure that the security policies are kept in place at the Account Level. How can you achieve this? Choose 2 answers from the options given below

- A. Use AWS organizations
- B. Club all divisions under a single account instead

C. Use IAM Policies to segregate access

D. Use Service control policies

---

**Explanation:**

Answer - A and D

With AWS Organizations, you can centrally manage policies across multiple AWS accounts without having to use custom scripts and manual processes. For example, you can apply service control policies (SCPs) across multiple AWS accounts that are members of an organization. SCPs allow you to define which AWS service APIs can and cannot be executed by AWS Identity and Access Management (IAM) entities (such as IAM users and roles) in your organization's member AWS accounts. SCPs are created and applied from the master account, which is the AWS account that you used when you created your organization.

Option B is incorrect since the question mentions that you need to use separate AWS accounts

Option C is incorrect since you need to use service control policies."AWS IAM doesn't provide the facility to define access permissions to that minute level i.e., which AWS service APIs can and cannot be executed by IAM entities."

For more information on how to use service control policies, please visit the below URL

<https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-in-aws-organizations/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 24

Unattempted

Domain :Design Resilient Architectures

Your company has a set of EC2 Instances hosted on the AWS Cloud. As an architect, you have been told to ensure that if the status of any of the instances is related to failure, then the instances should restart automatically. How can you achieve this in the most efficient way possible?

- A. Create CloudWatch alarms that stop and start the instance based off of status check alarms
- B. Write a script that queries the EC2 API for each instance status check
- C. Write a script that periodically shuts down and starts instances based on certain stats.
- D. Implement a third-party monitoring tool.

---

**Explanation:**

Answer – A

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

All other options are possible , but would just be an extra maintenance overhead

For more information on using alarm actions, please refer to the below link

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

**View Queries**

open ▾

Question 25

Unattempted

Domain :Design Secure Applications and Architectures

You are working for a financial institute using AWS cloud infrastructure. All project related data is uploaded to Amazon EFS. This data is retrieved from on-premises data centre connecting to VPC via AWS Direct Connect. You need to ensure that all client access to EFS is encrypted using TLS 1.2 to

adhere to latest security guidelines issued by security team. Which of the following is cost effective recommended practice for securing data in transit while accessing data from Amazon EFS?

- A. Use EFS mount helper to encrypt data in transit.
- B. Use stunnel to connect to Amazon EFS & encrypt traffic in transit.
- C. Use third-party tool to encrypt data in transit.
- D. Use NFS client to encrypt data in transit.

---

**Explanation:****Correct Answer – A**

While mounting Amazon EFS, if encryption of data in transit is enabled, EFS Mount helper initializes the client Stunnel process to encrypt data in transit. EFS Mount helper uses TLS 1.2 to encrypts data in transit.

Option B is incorrect as using stunnel for encryption of data in transit will work fine, but there would be additional admin work to download & install stunnel for each mount.

Option C is incorrect as using a third-party tool will be a costly option.

Option D is incorrect as NFS client can't be used to encrypt data in transit. The amazon-efs-utils package can be used which consists of an EFS mount helper.

For more information on encrypting of data in transit for EFS, refer to the following URL,

<https://docs.aws.amazon.com/efs/latest/ug/encryption-in-transit.html#encrypt-mount>

---

Ask our Experts

Rate this Question? 😊 😞

---

**View Queries**

open ▾

Question 26

Unattempted

Domain :Design Secure Applications and Architectures

Your company has a set of resources defined in AWS. These resources consist of applications hosted on EC2 Instances. Data is stored on EBS volumes and S3. The company mandates that all data should

be encrypted at rest. How can you achieve this? Choose 2 answers from the options below

- A. Enable SSL with the underlying EBS volumes
- B. Enable EBS Encryption
- C. Make sure that data is transmitted from S3 via HTTPS
- D. Enable S3 server-side Encryption

---

**Explanation:**

Answer - B and D

The AWS Documentation mentions the following

Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure.

Server-side encryption protects data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) uses strong multi-factor encryption.

Options A and C are incorrect since these have to do with encryption of data in transit and not encryption of data at rest

For more information on EBS Encryption, please refer to the below link

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

For more information on S3 server-side encryption, please refer to the below link

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html>

---

Ask our Experts

Rate this Question? 😊 😞



## View Queries

## Question 27

Unattempted

Domain :Design Secure Applications and Architectures

Your company has a web application hosted in AWS that makes use of an Application Load Balancer. You need to ensure that the web application is protected from web-based attacks such as cross site scripting etc.

Which of the following implementation steps can help protect web applications from common security threats from the outside world?

- A. Place a NAT instance in front of the web application to protect against attacks
- B. Use the WAF service in front of the web application
- C. Place a NAT gateway in front of the web application to protect against attacks
- D. Place the web application in front of a CDN service instead

---

**Explanation:**

Answer – B

The AWS Documentation mentions the following

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

Options A and C are incorrect because these are used to allow instances in your private subnet to communicate with the internet

Option D is incorrect since this is ideal for content distribution and good when you have DDos attacks , but the WAF should be used for concentrated types of web attacks

For more information on AWS WAF, please refer to the below link

<https://aws.amazon.com/waf/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 28

Unattempted

Domain :Design High-Performing Architectures

Your supervisor asks you to create a decoupled application whose process includes dependencies on EC2 instances where you would be using Polling Strategy to trigger messages once the defined criteria are fulfilled. Which of the following would you include in the architecture?

- A. An SQS queue as the messaging component between the Instances and servers
- B. An SNS topic as the messaging component between the Instances and servers
- C. An Elastic Load balancer to distribute requests to your EC2 Instance
- D. Route 53 resource records to route requests based on failure

---

**Explanation:**

Answer – A

The AWS Documentation mentions the following

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

**SQS** is a distributed **queuing** system. Messages are NOT pushed to receivers. Receivers have to **poll** or **pull** messages from **SQS**

**SNS** is a distributed **publish-subscribe** system. Messages are **pushed** to subscribers as and when they are sent by publishers to SNS.

Option B is incorrect since this is a push-based notification service

Option C is incorrect since there is no mention in the question of adding any fault tolerance

Option D is incorrect since there is no mention in the question of adding any failure detection

For more information on AWS SQS, please refer to the below link

<https://aws.amazon.com/sqs/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 29

Unattempted

Domain :Design High-Performing Architectures

Your company has a set of VPC's. There is now a requirement to establish communication across the Instances in the VPC's. Your supervisor has asked you to implement the VPC peering connection. Which of the following considerations would you keep in mind for VPC peering. Choose 2 answers from the options below

- A. Ensuring that the VPC's don't have overlapping CIDR blocks
- B. Ensuring that no on-premises communication is required via transitive routing
- C. Ensuring that the VPC's only have public subnets for communication
- D. Ensuring that the VPC's are created in the same region

---

**Explanation:**

Answer - A and B

The AWS Documentation mentions the following with restrictions for VPC peering

## Overlapping CIDR Blocks

You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.

### Overlapping CIDR Blocks

You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.



Transitive peering is unsupported for VPC Peering

Option C is incorrect since it is not necessary that the VPC's only contain public subnets

Option D is incorrect since it is not necessary that the VPC's are created in the same region

For more information on Invalid peering configurations, please refer to the below link

<https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html>

**Note:** AWS now supports VPC Peering across different regions. Please check below AWS Docs for more details:

<https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/>

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

Question 30

Unattempted

Domain :Design High-Performing Architectures

You have been instructed to establish a successful site-to-site VPN connection from your on-premises network to the VPC (Virtual Private Cloud). As an architect, which of the following pre-requisites should you ensure are in place for establishing the site-to-site VPN connection. Choose 2 answers from the options given below

- A. The main route table to route traffic through a NAT instance
- B. A public IP address on the customer gateway for the on-premises network
- C. A virtual private gateway attached to the VPC
- D. An Elastic IP address to the Virtual Private Gateway

---

**Explanation:**

Answer - B and C

This is mentioned in the AWS Documentation

## Virtual Private Gateway

A *virtual private gateway* is the VPN concentrator on the Amazon side of the VPN connection. You create a virtual private gateway and attach it to the VPC from which you want to create the VPN connection.

When you create a virtual private gateway, you can specify the private Autonomous System Number (ASN) for the Amazon side of the gateway. If you don't specify an ASN, the virtual private gateway is created with the default ASN (64512). You cannot change the ASN after you've created the virtual private gateway. To check the ASN for your virtual private gateway, view its details in the **Virtual Private Gateways** screen in the Amazon VPC console, or use the [describe-vpn-gateways](#) AWS CLI command.

### Note

If you create your virtual private gateway before 2018-06-30, the default ASN is 17493 in the Asia Pacific (Singapore) region, 10124 in the Asia Pacific (Tokyo) region, 9059 in the EU (Ireland) region, and 7224 in all other regions.

## Customer Gateway

A *customer gateway* is a physical device or software application on your side of the VPN connection.

To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. The following table describes the information you'll need to create a customer gateway resource.

| Item  | Description  |
|---|--|
| Internet-routable IP address (static) of the customer gateway's external interface. | The public IP address value must be static. If your customer gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device, and adjust your firewall rules to unblock UDP port 4500. |

Option A is incorrect since NAT instance is not required to route traffic via the VPN connection

Option D is incorrect the Virtual Private Gateway is managed by AWS

For more information on VPN connections, please refer to the below link

<https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html>

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ✓

Question 31

Unattempted

Domain :Design Secure Applications and Architectures

Your company wants to enable encryption of services such as S3 and EBS volumes so that the data it maintains is encrypted at rest. They want to have complete control over the keys ( including hardware ) and the entire lifecycle around the keys. How can you accomplish this?

- A. Use the AWS CloudHSM
- B. Use the KMS service
- C. Enable S3 server-side encryption
- D. Enable EBS Encryption with the default KMS keys

**Explanation:**

Answer – A

This is mentioned in the AWS Documentation

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs

KMS is a shared hardware tenancy - your keys are in their own partition of an encryption module shared with other AWS customers, each with their own isolated partition. Cloud HSM gives you your own hardware module, so the most likely reason to choose Cloud HSM is if you had to ensure your keys were isolated on their own encryption module.

Options B, C, and D are incorrect since they have shared hardware tenancy.

For more information on cloud HSM and Encryption Tools, please refer to the below URL

<https://aws.amazon.com/cloudhsm/>

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 32

Unattempted

Domain :Design High-Performing Architectures

A company wants to implement a data store in AWS. The data store needs to have the following requirements

- 1) Completely managed by AWS
  - 2) Ability to store JSON objects efficiently
  - 3) Scale based on demand
- Which of the following would you use as the data store?

- A. AWS Redshift
- B. AWS DynamoDB
- C. AWS Aurora
- D. AWS Glacier

---

**Explanation:**

Answer – B

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database so that you don't have to worry about hardware provisioning, setup, and configuration, replication, software patching, or cluster scaling. It is ideal for storing JSON based objects

With DynamoDB On-Demand, capacity planning is a thing of the past. You don't specify read and write capacity at all—you pay only for the usage of your DynamoDB tables. I pay more when I have more



usage, which means I'm delivering more value to my customers.

Previously, you had to set read and write throughput capacity on your DynamoDB tables. This specified how many and how large of reads and writes you could make on your table in any given second. Read and write capacity units were charged by the hour, and your requests would be throttled if you exceeded your provisioned capacity in any given second.

Option A is incorrect since this is normally used to host a data warehousing solution

Option C is incorrect since this doesn't provide scaling on-demand.

Option D is incorrect since this is used for archive storage

For more information on DynamoDB, please refer to the below link

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

<https://aws.amazon.com/blogs/aws/amazon-dynamodb-on-demand-no-capacity-planning-and-pay-per-request-pricing/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 33

Unattempted

Domain :Design Secure Applications and Architectures

A company has set up some EC2 Instances in a VPC with the default Security group and NACL settings. They want to ensure that the IT admin staff can connect to the EC2 Instance via SSH. As an architect what would you ask the IT admin team to do to ensure that they can connect to the EC2 Instance from the Internet? Choose 2 answers from the options below

- A. Ensure that the Instance has a Public or Elastic IP
- B. Ensure that the Instance has a Private IP
- C. Ensure to modify the Security groups
- D. Ensure to modify the NACL rules

**Explanation:**

Answer - A and C

The AWS Documentation mentions the following

To enable access to or from the internet for instances in a VPC subnet, you must do the following:

Attach an Internet gateway to your VPC.

Ensure that your subnet's route table points to the internet gateway.

Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address)

Ensure to add an inbound rule to allow traffic from SSH with source 0.0.0.0/0. By default, all outbound traffic is allowed

Option B is incorrect since the Private IP will always be created, and would not be used to connect from the internet

If you use the private IP to communicate, traffic will stay within the VPC, it will not be routed out, the routing table will route it internally

If you use the public IP to communicate, traffic will go out to the internet (through internet gateway) and come back to your VPC

Instances receive a Public IP address so that it is reachable from *outside* the VPC. This IP address might change if the instance stops and starts. Alternatively, you can use an Elastic IP Address that remains static.

Option D is incorrect since the default NACL rules will allow all traffic

For more information on exposing VPC resources to the Internet please refer to the below link

[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html)

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 34

Unattempted

Your company has a set of EBS volumes and a set of adjoining EBS snapshots. They want to minimize the costs for the underlying EBS snapshots. Which of the following approaches provides the lowest cost for Amazon Elastic Block Store snapshots while giving you the ability to fully restore data?

- A. **Maintain two snapshots: the original snapshot and the latest incremental snapshot.**
- B. **Maintain a volume snapshot; subsequent snapshots will overwrite one another**
- C. **Maintain a single snapshot: the latest snapshot is both Incremental and complete.**
- D. **Maintain the most current snapshot, archive the original and incremental to Amazon Glacier.**

---

**Explanation:**

Answer – C

The AWS Documentation mentions the following

You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume.

For more information on EBS Snapshots, please refer to the below link

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 35

Unattempted

**Domain :Design High-Performing Architectures**

You are using a c5.large EC2 Instance with one 300GB EBS General purpose SSD volume to host a relational database. You noticed that the read/write capacity of the database needs to be increased. Which of the following approaches can help achieve this? Choose 2 answers from the options given below.

- A. Use a larger EC2 Instance Type
- B. Enable Multi-AZ feature for the database.
- C. Consider using Provisioned IOPS Volumes.
- D. Put the database behind an Elastic Load Balancer.

---

**Explanation:**

Answer - A and C

The below snapshot from the AWS Documentation shows the different volume types and why Provisioned IOPS is the most ideal for this requirement

## Amazon EBS Volume Types

The following table shows use cases and performance characteristics of current generation EBS volumes:

| Volume Type       | Solid State Drives (SSD)  |  | Hard Disk Drives (HDD)   |  |
|-------------------|---|--|--|--|
|                   | EBS Provisioned IOPS SSD (io1)  | EBS General Purpose SSD (gp2)*   | Throughput Optimized HDD (st1)   | Cold HDD (sc1)   |
| Short Description | Highest performance SSD volume designed for latency-sensitive transactional workloads | General Purpose SSD volume that balances price performance for a wide variety of transactional workloads | Low cost HDD volume designed for frequently accessed, throughput intensive workloads | Lowest cost HDD volume designed for less frequently accessed workloads |

Also, consider using a larger instance size for better processing capabilities based on EBS Bandwidth

Option B is incorrect since the Multi-AZ feature is only for high availability

Option D is incorrect since this would not alleviate the high number of read/write of the database

For more details on EBS Volume Types and EC2 Instance Types, please refer below URL

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#EBSVolumeTypes\\_piops](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html#EBSVolumeTypes_piops)

<https://aws.amazon.com/ec2/instance-types/>

Ask our Experts

Rate this Question? 😊 😞

## Question 36

Unattempted

## Domain :Design Cost-Optimized Architectures

Your company has a set of AWS RDS Instances. Your management has asked you to disable Automated backups to save on cost. When you disable automated backups for AWS RDS, what are you compromising on?

- A. Nothing, you are actually saving resources on aws
- B. You are disabling the point-in-time recovery.
- C. Nothing really, you can still take manual backups.
- D. You cannot disable automated backups in RDS.

**Explanation:**

Answer – B

Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. You can set the backup retention period when you create a DB instance. If you don't set the backup retention period, Amazon RDS uses a default period retention period of one day. You can modify the backup retention period; valid values are 0 (for no backup retention) to a maximum of 35 days.

Automatic Backups are taken daily at whichever time we specify, the point in time recovery feature enables to recover the database at any point in time and AWS applies the transaction logs to the most appropriate DB backup. Whereas DB snapshots are a manual thing where we user manually triggers the backup and then restores it from the desired time period.

You will also specifically see AWS mentioning the risk of not allowing automated backups.

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_WorkingWithAutomatedBackups.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html)

**Important**

We highly discourage disabling automated backups because it disables point-in-time recovery. If you disable and then re-enable automated backups, you are only able to restore starting from the time you re-enabled automated backups.

Manual snapshots are user-initiated backups of your instance stored in Amazon S3 that are kept until you explicitly delete them. You can create a new instance from a database snapshot whenever you

desire. Although database snapshots serve operationally as full backups, you are billed only for incremental storage use.

Because of the risk which is clearly mentioned in the AWS Documentation, all other options are incorrect.

For more information on Automated backups, please visit

[http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_WorkingWithAutomatedBackups.ht](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.ht)

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 37

Unattempted

Domain :Design High-Performing Architectures

A company is planning on setting up a web-based application. They need to ensure that users across the world have the ability to view the pages from the web site with the least amount of latency. How can you accomplish this?

- A. Use Route 53 with latency-based routing
- B. Place a cloudfront distribution in front of the web application
- C. Place an Elastic Load balancer in front of the web application
- D. Place an Elastic Cache in front of the web application

---

**Explanation:**

Answer – B

The AWS Documentation mentions the following

Amazon CloudFront is a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to your viewers with low latency and high transfer speeds. CloudFront is integrated with AWS – including physical locations that are directly connected to the AWS global infrastructure, as well as software that works seamlessly with services including AWS Shield for DDoS

mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code close to your viewers.

## CloudFront vs Route 53

**CloudFront** will distribute your content over 100+ edge location which will decrease your response time with low latency and save your cost as well. It will deliver the content from the nearest location.

**CloudFront:** It is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. The content is cached at the edge location (data center). In CloudFront, you specify the distribution from where the content needs to be served.

**Route53** is a DNS service and is an origin of data. The term Origin is a term for where the original data resides before it is cached in the CDN (CloudFront). It redirects the original content rather than caching.

Option A can be correct but the least amount of latency will not be there.

Option C is incorrect since this is used for fault tolerance for the web application

Option D is incorrect since this is used for caching requests in front of a database layer

For more information on AWS CloudFront, please visit

<https://aws.amazon.com/cloudfront/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 38

Unattempted

Domain :Design High-Performing Architectures

A company is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The customer also uses Amazon Route 53 to manage its public DNS. How should Route 53 be configured to ensure the custom domain is made to point to the load balancer and it should be cost-effective? Choose 2 answers from the options below.



- A. Don't go for Route 53, choose third party service.
- B. Create a CNAME record pointing to the load balancer
- C. Create an alias record pointing to the load balancer.
- D. Ensure that a hosted zone is in place

---

**Explanation:**

Answer - C and D

The AWS Documentation mentions the following

While ordinary Amazon Route 53 records are standard DNS records, alias records provide a Route 53-specific extension to DNS functionality. Instead of an IP address or a domain name, an alias record contains a pointer to an AWS resource such as a CloudFront distribution or an Amazon S3 bucket. When Route 53 receives a DNS query that matches the name and type in an alias record, Route 53 follows the pointer and responds with the applicable value:

If you host a website on multiple Amazon EC2 instances, you can distribute traffic to your website across the instances by using an Elastic Load Balancing (ELB) load balancer. The ELB service automatically scales the load balancer as traffic to your website changes over time. The load balancer also can monitor the health of its registered instances and route domain traffic only to healthy instances.

To route domain traffic to an ELB load balancer, use Amazon Route 53 to create an alias record that points to your load balancer. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as example.com and for subdomains, such as www.example.com. (You can create CNAME records only for subdomains.)

Route 53 doesn't charge for alias queries to ELB load balancers or other AWS resources.

Options A is incorrect since it will cost you more

Option B can be correct as well but that is not cost-effective.

Option D is correct because Hosted Zone - is a container for records, and records contain information about how you want to route traffic for a specific domain, such as example.com, and its subdomains (vpc.example.com, elb.example.com). A hosted zone and the corresponding domain have the same name.

For more information on the procedure, please visit below URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/using-domain-names-with-elb.html#dns-associate-custom-elb>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 39

Unattempted

Domain :Design High-Performing Architectures

A company is hosting their website on a cluster of web servers that are behind a public-facing load balancer. The web application interacts with an AWS RDS database. It has been noticed that a set of similar types of queries is causing a performance bottleneck at the database layer. Which of the following architecture additions can help alleviate this issue?

- A. Deploy ElastiCache in front of the web servers
- B. Deploy ElastiCache in front of the database servers
- C. Deploy Elastic Load balancer in front of the web servers
- D. Enable Multi-AZ for the database

---

**Explanation:**

Answer – B

The AWS Documentation mentions the following

Amazon ElastiCache offers fully managed **Redis** and **Memcached**. Seamlessly deploy, operate, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores

Option A is incorrect since the database is having issues hence you need to ensure that ElastiCache is placed in front of the database servers

Option C is incorrect since there is an issue with the database servers, so we don't need to add anything for the web servers

Option D is incorrect since this is used for high availability of the database

For more information on ElastiCache, please visit

<https://aws.amazon.com/elasticache/>

---

## Try now labs related to this question

### Introduction to AWS Elastic Load Balancing

This lab walks you through AWS Elastic Load Balancing. Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. In this lab, we will demonstrate elastic load balancing with 2 EC2 Instances.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 40

Unattempted

Domain :Design Resilient Architectures

A company is hosting their website on a cluster of web servers that are behind a public-facing load balancer. The web application interfaces with an AWS RDS database. The management has specified that the database needs to be available in case of a hardware failure on the primary database. The secondary needs to be made available in the least amount of time. Which of the following would you opt for?

- A. Made a snapshot of the database
- B. Enabled Multi-AZ failover
- C. Increased the database instance size
- D. Created a read replica

---

### Explanation:

Answer – B

The AWS Documentation mentions the following

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete.

Options A and D are incorrect since even though they can be used to recover a database, it would just take more time than just enabling Multi-AZ

Option C is incorrect since this will not help the cause

For more information on Multi-AZ, please visit

<https://aws.amazon.com/rds/details/multi-az/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 41

Unattempted

Domain :Design High-Performing Architectures

Your company is planning on launching a set of EC2 Instances for hosting their production-based web application. As an architect, you have to instruct the operations department on which service they can use to trigger AWS Lambda based on real-time events. Which of the following would you recommend?

- A. AWS Cloudtrail
- B. AWS Cloudwatch
- C. AWS SQS
- D. AWS SNS

**Explanation:**

Answer – B

The AWS Documentation mentions the following

Amazon CloudWatch is a monitoring and management which collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications and services that run on AWS, and on-premises servers. It captures real-time events which can be further used to trigger AWS Lambda

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs. It doesn't have the capability to trigger anything.

For more details on the process, refer below URL

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-Rule.html>

Option C is incorrect since this is used to working with messages in the queue

Option D is incorrect since this is used for sending notifications

For more information on AWS CloudWatch, please visit the below URL

<https://aws.amazon.com/cloudwatch/>

**Try now labs related to this question****Using CloudWatch for Resource Monitoring, Create CloudWatch Alarms and Dashboards**

This lab walks you through the various CloudWatch features available which are used for resource monitoring.



**Credit Needed 10**



**Time 0 : 45**

[Try Now](#)

[Ask our Experts](#)

Rate this Question?



## View Queries

open ▾

## Question 42

Unattempted

## Domain :Design High-Performing Architectures

A company is planning on storing their files from their on-premises location onto the Simple Storage service. After a period of 3 months, they want to archive the files, since they would be rarely used. Which of the following would be the right way to service this requirement?

- A. Use an EC2 instance with EBS volumes. After a period of 3 months, keep on taking snapshots of the data.
- B. Store the data on S3 and then use Lifecycle policies to transfer the data to Amazon Glacier
- C. Store the data on Amazon Glacier and then use Lifecycle policies to transfer the data to Amazon S3
- D. Use an EC2 instance with EBS volumes. After a period of 3 months , keep on taking copies of the volume using Cold HDD volume type.

---

**Explanation:**

Answer – B

The AWS Documentation mentions the following

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

Transition actions—Define when objects transition to another storage class. For example, you might choose to transition objects to the STANDARD\_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.

Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

Options A and D are incorrect since using EBS volumes is not the right storage option for this sort of requirement

Option C is incorrect since the files should be initially stored in S3.

For more information on AWS S3 Lifecycle policies, please visit the below URL

---

## Try now labs related to this question

### How to enable versioning Amazon S3

This lab walks you through to the steps how to Enables Versioning to a AWS S3 Bucket. Versioning enables you to keep multiple versions of an object in one bucket. In this lab we learn how to enable object versioning on a S3 bucket.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 43

Unattempted

Domain :Design High-Performing Architectures

A company has a workflow that sends video files from their on-premise system to AWS for transcoding. They use EC2 worker instances that pull transcoding jobs from SQS. As an architect, you need to design how the SQS service would be used in this architecture in order to achieve high throughput. Which of the following is the ideal way in which the SQS service should be used?

- A. SQS should be used to guarantee high throughput because of the order of messages.
- B. SQS should be used to synchronously manage the transcoding output.
- C. SQS should be used to check the health of the worker instances.
- D. SQS should be used to facilitate horizontal scaling

---

**Explanation:**

Answer – D

The AWS Documentation mentions the following

Amazon Simple Queue Service (Amazon SQS) offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components.

Option A is incorrect since the ordering of messages won't help in achieving high throughput

Options B and C are incorrect since these are not the responsibility of the SQS queue

For more information on AWS SQS Horizontal Scaling, please visit the below URL

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-throughput-horizontal-scaling-and-batching.html#horizontal-scaling>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Question 44

Unattempted

Domain :Design Secure Applications and Architectures

You're an architect for your company. Your IT admin staff needs access to newly created EC2 Instances for administrative purposes. Which of the following needs to be done to ensure that the IT admin staff can successfully connect via port 22 on to the EC2 Instances

- A. Adjust Security Group to permit egress traffic over TCP port 443 from your IP.
- B. Configure the IAM role to permit changes to security group settings.
- C. Modify the instance security group to allow ingress of ICMP packets from your IP.
- D. Adjust the instance's Security Group to permit ingress traffic over port 22.
- E. Apply the most recently released Operating System security patches.

**Explanation:**

Answer - D



A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances.

For connecting via SSH on EC2, you need to ensure that port 22 is open on the security group for the EC2 instance.

Option A is wrong, because port 443 is for HTTPS and not for SSH.

Option B is wrong because IAM role is not pertinent to security groups

Option C is wrong because this is relevant to ICMP and not SSH

Option E is wrong because it does not matter what patches are there on the system

For more information on EC2 Security groups, please visit the url



<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html>

---

## Try now labs related to this question

### Introduction to Amazon Elastic Compute Cloud (EC2)

1. This lab walks you through the steps to launch and configure a virtual machine in the Amazon cloud.
2. You will practice using Amazon Machine Images to launch Amazon EC2 Instances and use key pairs for SSH authentication to log into your instance. You will create a web page and publish it.

 Credit Needed 10    Time 0 : 30

[Try Now](#)

[Ask our Experts](#)

Rate this Question? 😊 😞

[View Queries](#)[open](#) ▼

Question 45

Unattempted

Domain :Design Cost-Optimized Architectures

Your company is running a photo sharing website. Currently all the photos are stored in S3. At some point the company finds out that other sites have been linking to the photos on your site, causing loss to your business. You need to implement a solution for the company to mitigate this issue. Which of the following would you look at implementing?

- A. Remove public read access and use signed URLs with expiry dates.
- B. Use CloudFront distributions for static content.
- C. Block the IPs of the offending websites in Security Groups.
- D. Store photos on an EBS volume of the web server.

**Explanation:**

Answer - A

The AWS Documentation mentions the following

A pre-signed URL gives you access to the object identified in the URL, provided that the creator of the pre-signed URL has permission to access that object. That is, if you receive a pre-signed URL to upload an object, you can upload the object only if the creator of the pre-signed URL has the necessary permissions to upload that object.

Option B is incorrect since CloudFront is only used for the distribution of content across edge or region locations. It is not used for restricting access to content

Option C is incorrect since Blocking IP's is challenging because they are dynamic in nature and you will not know which sites are accessing your main site

Option D is incorrect since Storing photos on EBS volume is not a good practice or architecture approach for an AWS Solution Architect

For more information on serving private content please visit the URL

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 46

Unattempted

Domain :Design High-Performing Architectures

You have been hired as a consultant for a company to implement their CI/CD processes. They currently use an on-premises deployment of Chef for their configuration management on servers. You need to advise them on what they can use on AWS to leverage their existing capabilities. Which of the following service would you recommend?

- A. Amazon Simple Workflow Service
- B. AWS Elastic Beanstalk
- C. AWS CloudFormation
- D. AWS OpsWorks

---

**Explanation:**

Answer – D

The AWS Documentation mentions the following

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute

environments. OpsWorks has three offerings, AWS Opsworks for Chef Automate, AWS OpsWorks for Puppet Enterprise, and AWS OpsWorks Stacks.

All of the other options are incorrect since the only tool which works effectively with the Chef Configuration management tool is AWS OpsWorks.

For more information on AWS Opswork, please visit the url

<https://aws.amazon.com/opsworks/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 47

Unattempted

Domain :Design Secure Applications and Architectures

You are working as an AWS consultant for a banking institute. They have deployed a digital wallet platform for clients using multiple EC2 instances in us-east-1 region. The application establishes a secure encrypted connection between clients & EC2 instances for each transaction using custom TCP port 5810.

Due to the increasing popularity of this digital wallet, they are observing load on backend servers resulting in delay in transaction. For security purpose, all client IP address accessing this application should be preserved & logged. The technical team of banking institute is looking for a solution which will address this delay & also proposed solution should be compatible with millions of transactions done simultaneously. Which of the following is a recommended option to meet this requirement?

- A. Use Network Load Balancers with SSL certificate. Configure TLS Listeners on this NLB with custom security policy consisting of protocols & ciphers.
- B. Use Network Load Balancers with SSL certificate. Configure TLS Listeners on this NLB with default security policy consisting of protocols & ciphers.
- C. Use Network Load Balancers with SSL certificate. Configure TLS Listeners on this NLB with default security policy consisting of protocols & TCP port 5810.
- D. Use Network Load Balancers with SSL certificate. Configure TLS Listeners on this NLB with custom security policy consisting of protocols & TCP port 5810.

**Explanation:****Correct Answer – B**

Network Load Balancer can be used to terminate TLS connections instead of back end instance reducing the load on this instance. With Network Load Balancers, millions of simultaneous sessions can be established with no impact on latency along with preserving client IP address. To negotiate TLS connections with clients, NLB uses a security policy which consists of protocols & ciphers.

Option A is incorrect as Network Load Balancers does not support custom security policy

Option C is incorrect as Network Load Balancers should consist of security policies comprising of Protocols & Ciphers.

Option D is incorrect as Network Load Balancers does not support custom security policy as well as security policies should comprise of protocols & ciphers.

For more information on Security Policies for TLS termination on Network Load Balancers, refer to the following URL,

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

Ask our Experts

Rate this Question? 😊 😞

**View Queries**

open ▼

**Question 48**

**Unattempted**

**Domain :Design High-Performing Architectures**

You work as an architect for a company. There is a requirement for an application to be deployed on a set of EC2 Instances. These would be part of a compute cluster that requires low inter-node latency. Which of the following would you use for this requirement?

- A. Multiple Availability Zones
- B. AWS Direct Connect
- C. EC2 Dedicated Instances
- D. Cluster placement Groups
- E. VPC private subnets

**Explanation:**

Answer – D

The AWS Documentation mentions the following

Amazon Web Services' solution to reducing latency between instances involves the use of placement groups. As the name implies, a placement group is just that -- a group. AWS instances that exist within a common availability zone can be grouped into a placement group. Group members are able to communicate with one another in a way that provides low latency and high throughput.

Cluster Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both, and if the majority of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking

Because of what is mentioned in the documentation, all other options are incorrect

For more information on AWS placement groups, please visit the URL

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Ask our Experts

Rate this Question? 😊 😞

**View Queries**

open ✓

Question 49

Unattempted

Domain :Design High-Performing Architectures

Your company stores a large set of files in Amazon S3. They need to ensure that if any new files are added to an S3 bucket, an event notification would be sent to the IT admin staff. Which of the following could be used to fulfil this requirement? Choose 2 answers from the options given below.

A. Create an SNS topic

- B. Create an SQS queue
- C. Add an event notification to the S3 bucket
- D. Add an event notification to the S3 object

---

**Explanation:**

Answer - A and C

The AWS Documentation mentions the following

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

Go in S3 bucket properties then events and choose the relevant event and select send to as SNS topic

### Transfer acceleration

Enable fast, easy and secure transfers of files to and from your bucket.

[Learn more](#)

☐ Suspended

### Events

[+ Add notification](#) [Delete](#) [Edit](#)

| Name      | Events | Filter | Type |
|-----------|--------|--------|------|
| New event |        |        |      |

**Name** ⓘ

**Events** ⓘ

☐ PUT  
☐ POST  
☐ COPY  
☐ Multipart upload completed  
☐ All object create events  
☐ Object in RRS lost  
☐ Permanently deleted  
☐ Delete marker created

☐ All object delete events  
☐ Restore initiated  
☐ Restore completed  
☐ Replication time missed threshold  
☐ Replication time completed after threshold  
☐ Replication time not tracked  
☐ Replication failed

**Prefix** ⓘ

**Suffix** ⓘ

**Send to** ⓘ

Select notification destination ▼

- SNS Topic
- SQS Queue
- Lambda Function

☐ 0 Active notifications

[Cancel](#) [Save](#)

### Requester pays

The requester (instead of the bucket owner) will pay for requests and data transfer.

[Learn more](#)

☐ Disabled

Option B is incorrect since you need to create an SNS topic that could be used to send an email to multiple IT administrators

Option D is incorrect since the event notification needs to be placed on the bucket and not the object

**NOTE:**

**Options C and D are different.**

**Option C:** Add an event notification to the **S3 bucket**

**Option D:** Add an event notification to the **S3 object**



For more information on AWS S3 notifications, please visit the URL

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>

## Try now labs related to this question

### Creating and Subscribing to SNS Topics, Adding SNS event for S3 bucket

This lab walks you through the creation and subscription of an Amazon SNS Topic. Using AWS S3 bucket you will test the subscription.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Question 50

Unattempted

Domain :Design High-Performing Architectures

Your company is planning on migrating code written in C# from their on-premises infrastructure onto AWS. They want to ensure to limit the amount of maintenance that would be required for the underlying infrastructure. Which of the following would they choose for hosting the code base?

- A. AWS Lambda
- B. AWS EC2
- C. AWS ECS
- D. AWS SQS

### Explanation:

Answer – A

The AWS Documentation mentions the following

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume - there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service - all with zero administration

With Lambda you don't need to build, secure, or maintain a container. You just worry about the code

**EC2** - is simply a remote (virtual) machine.

ECS stands for Elastic Container Service. ECS is basically a logical grouping of **EC2** Instances. Technically, ECS is a mere configuration for the efficient use and management of your **EC2** instance(s) resources i.e. storage, memory, CPU, etc.

To simplify it further, if you have launched an Amazon ECS with no **EC2** instances added to it, it's good for nothing i.e. you can't do anything about it. **ECS** makes sense only once one (or more) **EC2** instances are added to it.

Options B and C are incorrect since here you would need to manage the underlying servers

Option D is incorrect since this is a messaging service

For more information on AWS Lambda, please visit the URL

<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

---

## Try now labs related to this question

### Introduction to Amazon Lambda

This lab walks you through creation and usage of AWS Serverless service called AWS Lambda. In this lab, we will create a sample lambda function which is triggered on S3 Object upload event and makes a copy of that object on another S3 Bucket.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

## Question 51

Unattempted

## Domain :Design High-Performing Architectures

A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. There is a requirement to ensure that instances in the Development and Test VPC's can access resources in the Production VPC for a limited amount of time. Which of the following would be the ideal way to get this in place?

- A. Create an AWS Direct Connect connection between the Development, Test VPC to the Production VPC
- B. Create a separate VPC peering connection from Development to Production and from Test to the Production VPC
- C. Create a VPN connection between the Development, Test VPC to the Production VPC
- D. Create a VPC peering connection between the Development to the Production VPC and from Development to the Test VPC.

---

**Explanation:**

Answer – B

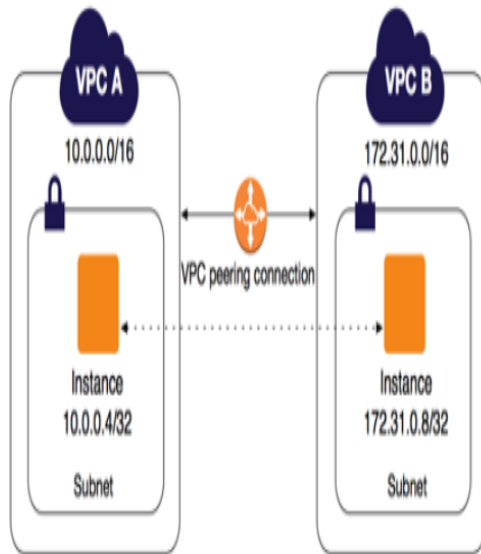
Options A and C are incorrect since this is only required for a short duration of time, hence you need to choose VPC peering

Options D is incorrect since the VPC Peering configuration mentioned would be invalid.

You need VPC Peering Configuration between Dev to Prod and Test to Prod

"A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection)."

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an *inter-region* VPC peering connection).



For more information on VPC peering please visit the URL

<https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/Welcome.html>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Question 52

Unattempted

Domain :Design High-Performing Architectures

You are designing the application architecture for a company. The architecture is going to consist of a web tier that will be hosted on EC2 Instances placed behind an Elastic Load Balancer. Which of the following would be considered as the basic requirements for the components of the application architecture? Choose 2 options:

- A. Determine the required I/O operations
- B. Determining the minimum memory requirements for an application
- C. Determining where the traffic has to be routed.
- D. Determining what all licenses Client require for their applications in Instance

---

**Explanation:**

Answer - A and B

You should decide on what are requirements for the underlying EC2 Instance. You can then choose the Instance type for the underlying EC2 Instance

Option C is incorrect since the ELB will take care of the distribution of traffic

Option D is incorrect since this is not considered as basic requirement as it is something required inside the Instance

For more information on EC2 Instance types, please visit the URL

<https://aws.amazon.com/ec2/instance-types/>

---

Ask our Experts

Rate this Question? 😊 😞

---

**View Queries**

open ▼

**Question 53**

**Unattempted**

**Domain :Design Resilient Architectures**

Your company has a requirement to host an application in AWS that requires access to a NoSQL database. But there are no human resources available who can take care of the database infrastructure. In addition to this, the database should have the capability to scale automatically based on demand and also have high availability. Which of the following databases would you use for this purpose?

- A. **DynamoDB**
- B. **ElasticMap Reduce**
- C. **Amazon RDS**
- D. **Amazon Aurora**

---

**Explanation:**

Answer – A

The AWS Documentation mentions the following

Amazon DynamoDB is a nonrelational database that delivers reliable performance at any scale. It's a fully managed, multi-region, multi-master database that provides consistent single-digit millisecond latency, and offers built-in security, backup and restore, and in-memory caching.

With DynamoDB On-Demand, capacity planning is a thing of the past. You don't specify read and write capacity at all—you pay only for the usage of your DynamoDB tables. This fits perfectly with the Lambda and Serverless model—I pay more when I have more usage, which means I'm delivering more value to my customers.

Previously, you had to set read and write throughput capacity on your DynamoDB tables. This specified how many and how large of reads and writes you could make on your table in any given second. Read and write capacity units were charged by the hour, and your requests would be throttled if you exceeded your provisioned capacity in any given second.

Option B is invalid since this is used for Big Data

Option C is invalid since here you still have to partially manage the infrastructure

Option D is invalid since this would allow you to host MySQL compatible databases

For more information on DynamoDB, please visit the URL

<https://aws.amazon.com/dynamodb/>

---

Ask our Experts

Rate this Question?  

---

**View Queries**

open 

## Question 54

Unattempted

## Domain :Design Secure Applications and Architectures

You are working as an AWS consultant for an online grocery store. They are using two-tier web application with web-servers hosted in VPC's at us-east-1 region & on-premise data-centre. Network Load balancer is configured in front end to distribute traffic between these servers. All traffic between clients & servers is encrypted. To reduce load on back-end servers , they are looking for an alternate solution to terminate TLS connection on this Network Load balancer.

Management team of this store has engaged you for suggesting a solution for certificate management used in case of TLS termination. Which of the following is preferred secure option to provision & store certificates to be used along with Network Load Balancer for terminating TLS?

- A. **Use multiple certificates per TLS listener & If a hostname provided by a client matches multiple certificates in the certificate list, the load balancer selects all of the certificates**
- B. **Use TLS tools to generate a new certificate & upload in AWS Certificate Manager.**
- C. **Use a single certificate per TLS listener provided by AWS Certificate Manager.**
- D. **Use a single certificate with 4096 bits RSA keys for higher security.**

---

**Explanation:****Correct Answer – C**

Network Load Balancer requires one certificate per TLS connection to encrypt traffic between client & NLB , & forward decrypted traffic to target servers. Using AWS Certificate Manager is a preferred option, as these certificates are automatically renewed on expiry.

Option A is incorrect as Network Load Balancer uses a smart certificate selection algorithm with support for Server Name Indication (SNI). If the hostname provided by a client matches a single certificate in the certificate list, the load balancer selects this certificate. If a hostname provided by a client matches multiple certificates in the certificate list, the load balancer selects the best certificate that the client can support.

Refer section "Certificate List" under the link

: <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

Option B is incorrect as this will increase admin work. Also, you will need to monitor expiry dates of certificates & renew these certificates before expiration.

Option D is incorrect as Network Load Balancer do not support certificates with RSA bits higher than 2048 bits.

For more information on certificates for TLS termination on Network Load Balancers, refer to the following URL,

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

Question 55

Unattempted

Domain :Design Resilient Architectures

Your company is planning on moving to the AWS Cloud. One of the Web applications will be launched on a set of EC2 Instances. You need to ensure that the architecture is fault tolerant and highly available. Which of the following would be considered during the design process. Choose 2 answers from the options given below

- A. Have a Single Availability Zone for the databases
- B. Use a load balancer in front of the EC2 Instances
- C. Ensure that the EC2 Instances are spread across multiple availability zones
- D. Ensure that the EC2 Instances are spread across a single availability zone for better maintenance

#### Explanation:

Answer - B and C

This is clearly mentioned in the AWS Documentation

#### What Is Elastic Load Balancing?

Elastic Load Balancing distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in multiple Availability Zones. Elastic Load Balancing scales your load balancer as traffic to your application changes over time and can scale to the vast majority of workloads automatically.



## Load Balancer Benefits

A load balancer distributes workloads across multiple compute resources, such as virtual servers. Using a load balancer increases the availability and fault tolerance of your applications.

Option A is invalid because it will not increase the availability and fault tolerance of your applications

Option D is invalid because you need to ensure that the Instances are spread across multiple availability zones

For more information on load balancing and availability of EC2 Instances, please visit the URL

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 56

Unattempted

Domain :Design Resilient Architectures

You are working as an AWS Architect for a global IT firm. You need to set up a pilot blockchain project in the US East region using Amazon Managed Blockchain. You have created multiple nodes for this project to perform a secure transactions within the Blockchain network. Which of the following peer node will be used as Resource Endpoint to verify & complete transactions with other members?

- A. ResourceID.MemberID.NetworkID.managedblockchain.us-east-1.amazonaws.com:PortNumber
- B. NetworkID.MemberID.ResourceID.managedblockchain.us-east-1.amazonaws.com:PortNumber
- C. MemberID.NetworkID.ResourceID.managedblockchain.us-east-1.amazonaws.com:PortNumber
- D. MemberID.ResourceID.NetworkID.managedblockchain.us-east-1.amazonaws.com:PortNumber

**Explanation:****Correct Answer – A**

In AWS Managed Blockchain network, when any new member is created, a unique Id is assigned to these members. For any transaction between these members, each member should use following format

"ResourceID.MemberID.NetworkID.managedblockchain.AWSRegion.amazonaws.com:PortNumber".

Options B, C, & D are incorrect as format for resource endpoint is

"ResourceID.MemberID.NetworkID.managedblockchain.us-east-1.amazonaws.com:PortNumber"

For more information on AWS Blockchain concepts, refer to following URL,

<https://docs.aws.amazon.com/managed-blockchain/latest/managementguide/network-components.html>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▾

Question 57

Unattempted

Domain :Design Resilient Architectures

You are working for a start-up firm, working on a POC project, in which multiple EC2 instances are launched for an internal project to check Web application performance. During Test, you are observing a delay in new EC2 instance moving from booting to full load mode.

You perform another test to pre-warm EC2 instance by initiating EC2 instance into the desired mode & then moving to Hibernate state. You are looking for IP addressing changes post Hibernate state to provide this IP address details to Firewall Team. Which of the following is correct statement for IP address changes when EC2 instance is moved from Running state to Hibernate & back to Running state?

- A. Both Public IPv4 and Private IPv4 are allocated with new IP while any IPv6 is retained
- B. Only Public IPv4 is allocated with new IP while Private IPv4 and any IPv6 are retained.
- C. Only IPv6 is allocated with new IP while both Private IPv4 and Public IPv4 are retained.

- D. All IP addresses allocated to EC2 instance are released & new IP address is allocated to EC2 instance post hibernation.

---

**Explanation:****Correct Answer – B**

The instance retains its private IPv4 addresses and any IPv6 addresses when hibernated and started. AWS releases the public IPv4 address and assigns a new one when you start it.

Option A is incorrect as when the EC2 instance is hibernated & restarted, there is no change in Private IPv4 address assigned to EC2 instance.

Option C is incorrect as when the EC2 instance is hibernated & restarted, there is no change in Public IPv6 address assigned to EC2 instance.

Option D is incorrect as when the EC2 instance is hibernated & restarted, there is a change in Public IPv4 address assigned to EC2 instance while no change in Private IPv4 & IPv6 address assigned to EC2 instance.

For more information on IP Address for EC2 in Hibernate state, refer to the following URL,

[https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html#instance\\_hibernate](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html#instance_hibernate)

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 58

Unattempted

Domain :Design Resilient Architectures

As a solutions architect, it is your job to design for high availability and fault tolerance. Company-A is utilizing Amazon S3 to store large amounts of file data. You need to ensure that the files are still available in the case of an entire region facing an outage due to a natural disaster. How can you achieve this?

- A. Copy the S3 bucket to an EBS optimized backed EC2 instance

- B. Amazon S3 is highly available and fault tolerant by design and requires no additional configuration
- C. Enable Cross-Region Replication for the bucket
- D. Enable versioning for the bucket

---

**Explanation:**

Answer – C

The AWS Documentation mentions the following

Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions. We refer to these buckets as *source* bucket and *destination* bucket. These buckets can be owned by different AWS accounts.

AWS services are designed with DR considerations in mind. S3, for example, achieves 99.999999999% durability and 99.99% availability by redundantly storing data across multiple AZs within a region. It may be rare for the whole AWS region to go down, but it could cause massive permanent damage if we don't plan for it; this is when S3 **Cross-Region Replication (CRR)** solution comes into play.

Option A is invalid because this is not the right way to take backups of an S3 bucket

Option B is invalid because yes S3 will ensure objects are available in multiple availability zones but not across regions in case of a disaster

Option D is invalid because versioning can only help from accidental deletion of objects but not from disaster recovery

For more information on Cross-Region Replication, please visit the URL

<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

**NOTE:**

Most organizations try to implement High Availability (HA) instead of DR to guard them against any downtime of services. In case of HA, we ensure there exists a fallback mechanism for our services. The service that runs in HA is handled by hosts running in different availability zones but in the same geographical region. This approach, however, does not guarantee that our business will be up and running in case the entire region goes down. DR takes things to a completely new level, wherein you need to be able to recover from a different region that's separated by over 250 miles. Our DR implementation is an Active/Passive model, meaning that we always have minimum critical services

running in different regions, but a major part of the infrastructure is launched and restored when required.

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 59

Unattempted

Domain :Design Cost-Optimized Architectures

Your company currently has a set of virtual servers that need to be migrated to the AWS Cloud. These Instances are normally 70% utilized and used throughout the year. As a solutions architect which of the following Instance pricing model would you suggest?

- A. **Reserved instances**
- B. **On-demand instances**
- C. **Spot instances**
- D. **Regular instances**

---

**Explanation:**

Answer – A

The AWS Documentation mentions the following on the different instance pricing options

Amazon EC2 provides the following purchasing options to enable you to optimize your costs based on your needs:

On-Demand Instances – Pay, by the second, for the instances that you launch.

Reserved Instances – Purchase, at a significant discount, instances that are always available, for a term from one to three years.

Spot Instances – Request unused EC2 instances, which can lower your Amazon EC2 costs significantly.

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing

On-demand can be used but Reserved Instances are most cost-efficient in the given scenario

Option B is incorrect because Reserved Instances are more effective

Option C is incorrect because in Spot Instances Instance there is no commitment. As soon as the Bid price exceeds Spot price, a user gets the Instance. In an On-demand Instance, a user has to pay the On-demand rate specified by Amazon. Once they have bought the Instance they have to use it by paying that rate.

In Spot Instance, once the Spot price exceeds the Bid price, Amazon will shut the instance. The benefit to the user is that they will not be charged for the partial hour in which Instance was taken back from them.

Option D is incorrect because there is nothing like Regular Instances in AWS.

For more information on instance pricing options, please visit the URL

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▼

Question 60

Unattempted

Domain :Design High-Performing Architectures

Your company currently has a set of EC2 Instances hosted on the AWS Cloud. There is a requirement to ensure the restart of instances if a CloudWatch metric goes beyond a certain threshold. As a solutions architect, how would you ask the IT admin staff to implement this?

- A. Look at the Cloudtrail logs for events and then restart the Instance based on the events
- B. Create a CloudWatch metric which looks into the instance threshold, and assign this metric against an alarm to reboot the instance.
- C. Create a CLI script that restarts the server at certain intervals
- D. Use the AWS Config utility on the EC2 Instance to check for metrics and restart the server

**Explanation:**

Answer – B

The AWS Documentation mentions the following

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

Option A is incorrect because CloudTrail logs will provide event details and not metrics

Option C is incorrect because we want to restart Instance as we reach a certain threshold but this way it will keep on restarting the Instance even without any threshold reach

Option D is incorrect because AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources

For more information on using alarm actions, please visit the URL

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Question 61

Unattempted

Domain :Design High-Performing Architectures

You have a read-intensive application hosted in AWS. The application is currently using the MySQL RDS feature in AWS. The CloudWatch metrics are showing high read throughput on the database and are causing performance issues on the database. Which of the following can be used to reduce the read throughput on the MySQL database?

A. Enable the Multi-AZ on the MySQL RDS

- B. Use Cold Storage Volumes for the MySQL RDS
- C. Enable Read Replica
- D. Use SQS to queue up the reads

---

**Explanation:**

Answer – C

The AWS documentation mentions the following on Read Replica

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

Option A is invalid since this is used for fault tolerance for the database

Option B is invalid since this is not the ideal storage mechanism to use for databases which require high read throughput

Option D is invalid since SQS is used as a decoupling component and would not be the ideal fit to reduce the reads on the database

For more information on Read Replica, please visit the below URL:

<https://aws.amazon.com/rds/details/read-replicas/>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ▾

Question 62

Unattempted



## Domain :Design Cost-Optimized Architectures

You are working as an AWS Architect for a software company. You are working on a new project which involves an application, deployed on twenty C5 EC2 On-demand Instances with Elastic IP attached to each instance. During peak hours when you are initiating new instances, a considerable delay is observed. You perform a pilot test for the option of initiating these Instances and hibernating so that during peak hours, these instances could be quickly launched.

It works fine during a pilot phase and you are recommending this option to be implemented in production. The management team is concerned about the pricing of a large number of EC2 instances in the Hibernate state. What is considered to calculate the pricing for an EC2 instance in the Hibernate state?

- A. Elastic IP address and EBS volumes attached to EC2 Instance
- B. Total Compute capacity per hour, Elastic IP address and EBS volumes attached to EC2 Instance
- C. Total Compute capacity per hour and EBS volumes attached to EC2 Instance
- D. Total Compute capacity per hour & Elastic IP address attached to EC2 Instance

---

**Explanation:**

**Correct Answer – A**

When an EC2 instance is in the Hibernate state, you pay only for the EBS volumes and Elastic IP Addresses attached to it.

Options B, C, and D are incorrect because, when an EC2 instance is in hibernate state, compute capacity charges are not applicable. The charges are only applicable for the EBS volumes and Elastic IP Addresses attached to it.

For more information on pricing for an EC2 instance in Hibernate state, refer to the following URL:

<https://aws.amazon.com/blogs/aws/new-hibernate-your-ec2-instances/>

---

Ask our Experts

Rate this Question? 😊 😞

---

**View Queries**

open ▼

## Question 63

Unattempted

## Domain :Design High-Performing Architectures

Your company has started hosting their databases on the Amazon RDS. As an architect, they have requested you to advise the IT admin staff on what they should use to monitor the underlying databases and notifications should be sent to IT admin staff if any issues are detected. Which AWS services can accomplish these requirements? Choose 2 answers from the options given below.

- A. Amazon Simple Email Service
- B. Amazon CloudWatch
- C. Amazon Simple Queue Service (SQS)
- D. Amazon Route 53
- E. Amazon Simple Notification Service (SNS)

---

**Explanation:**

Answer - B and E

The AWS Documentation mentions the following

You can monitor DB instances using Amazon CloudWatch, which collects and processes raw data from Amazon RDS into readable, near real-time metrics. These statistics are recorded for a period of two weeks, so that you can access historical information and gain a better perspective on how your web application or service is performing.

Option A is invalid since this an email service and not a notification service

Option C is invalid since this is a queuing service

Option D is invalid since this is a domain name service

For more information on monitoring databases, please visit the below URL

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Monitoring.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Monitoring.html)

---

**Try now labs related to this question**

**Creating and Subscribing to SNS Topics, Adding SNS event for S3 bucket**

This lab walks you through the creation and subscription of an Amazon SNS Topic. Using AWS S3 bucket you will test the subscription.

💎 Credit Needed 10 ⌚ Time 0 : 30

Try Now

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Question 64

Unattempted

Domain :Design Cost-Optimized Architectures

Your company has started hosting their data store on AWS by using the Simple Storage service. They are storing files that are downloaded by users on a frequent basis. After a duration of 3 months, the files need to be transferred to archive storage since they are not used beyond this point. Which of the following could be used to effectively manage this requirement?

- A. Transfer the files via scripts from S3 to Glacier after a period of 3 months
- B. Use Lifecycle policies to transfer the files onto Glacier after a period of 3 months
- C. Use Lifecycle policies to transfer the files onto Cold HDD after a period of 3 months
- D. Create a snapshot of the files in S3 after a period of 3 months

**Explanation:**

Answer - B

The AWS Documentation mentions the following

To manage your objects so that they are stored cost-effectively throughout their lifecycle, configure their lifecycle. A *lifecycle configuration* is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

Transition actions—Define when objects transition to another **storage class**. For example, you might choose to transition objects to the STANDARD\_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.

Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf. The lifecycle expiration costs depend on when you choose to expire objects.

Option A is invalid since there is already the option of lifecycle policies

Option C is invalid since lifecycle policies are used to transfer to Glacier or S3-Infrequent Access

Option D is invalid since snapshots are used for EBS volumes

For more information on S3 lifecycle policies, please visit the below URL

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

---

Ask our Experts

Rate this Question? 😊 😞

---

View Queries

open ✓

Question 65

Unattempted

Domain :Design High-Performing Architectures

Your company is planning on setting up a VPC with private and public subnets and then hosting EC2 Instances in the subnet. It has to be ensured that instances in the private subnet can download updates from the internet. Which of the following needs to be part of the architecture for this requirement?

- A. WAF
- B. Direct Connect
- C. NAT Gateway
- D. VPN

**Explanation:**

Answer – C

The AWS Documentation mentions the following

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances

Option A is invalid since this is a web application firewall

Options B and D are invalid since these are used to connect on-premises infrastructure to AWS VPC's

For more information on NAT gateway, please visit the below URL

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html>

---

**Try now labs related to this question****Creating NAT Gateways in AWS**

This lab walks you through the steps to Create A NAT Gateway and allow internet access to Instance in Private Subnet.

💎 Credit Needed 10 ⌚ Time 0 : 45

Try Now

Ask our Experts

Rate this Question? 😊 😞

View Queries

open ▼

Finish Review

## Certification

[Cloud Certification](#)

[Java Certification](#)

[PM Certification](#)

[Big Data Certification](#)

## Support

[Contact Us](#)

[Help Topics](#)

## Company

[Become Our Instructor](#)

[Support](#)

[Discussions](#)

[Blog](#)

[Business](#)



## Join us on Slack!

Join our open **Slack community** and get your queries answered instantly! Our experts are online to answer your questions!

## Follow us



---

© Copyright 2020. Whizlabs Software Pvt. Ltd. All Right Reserved.