



- [🏠 \(https://www.whizlabs.com/learn\)](https://www.whizlabs.com/learn) > [My Courses \(https://www.whizlabs.com/learn/my-courses\)](https://www.whizlabs.com/learn/my-courses)  
> [AWS Certified Solutions Architect Associate \(https://www.whizlabs.com/learn/course/aws-csaa-practice-tests#section-1\)](https://www.whizlabs.com/learn/course/aws-csaa-practice-tests#section-1)  
> [CSAA Practice Test 5 \(https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14732\)](https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14732) > **Report**

## CSAA PRACTICE TEST 5

**Attempt** 7  
**Marks Obtained** 65 / 65  
**Your score is** 100%

**Completed on** Tuesday , 15 January 2019 , 11:34 AM  
**Time Taken** 01 H 25 M 13 S  
**Result** Pass

### Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Define Performant Architectures	16	16	0	0
2	Design Resilient Architectures	15	15	0	0
3	Define Operationally-Excellent Architectures	15	15	0	0
4	Design Cost-Optimized Architectures	11	11	0	0
5	Specify Secure Applications and Architectures	8	8	0	0

<b>65</b> Questions	<b>65</b> Correct	<b>0</b> Incorrect	<b>0</b> Unattempted
------------------------	----------------------	-----------------------	-------------------------

Show Answers

All	▼
-----	---

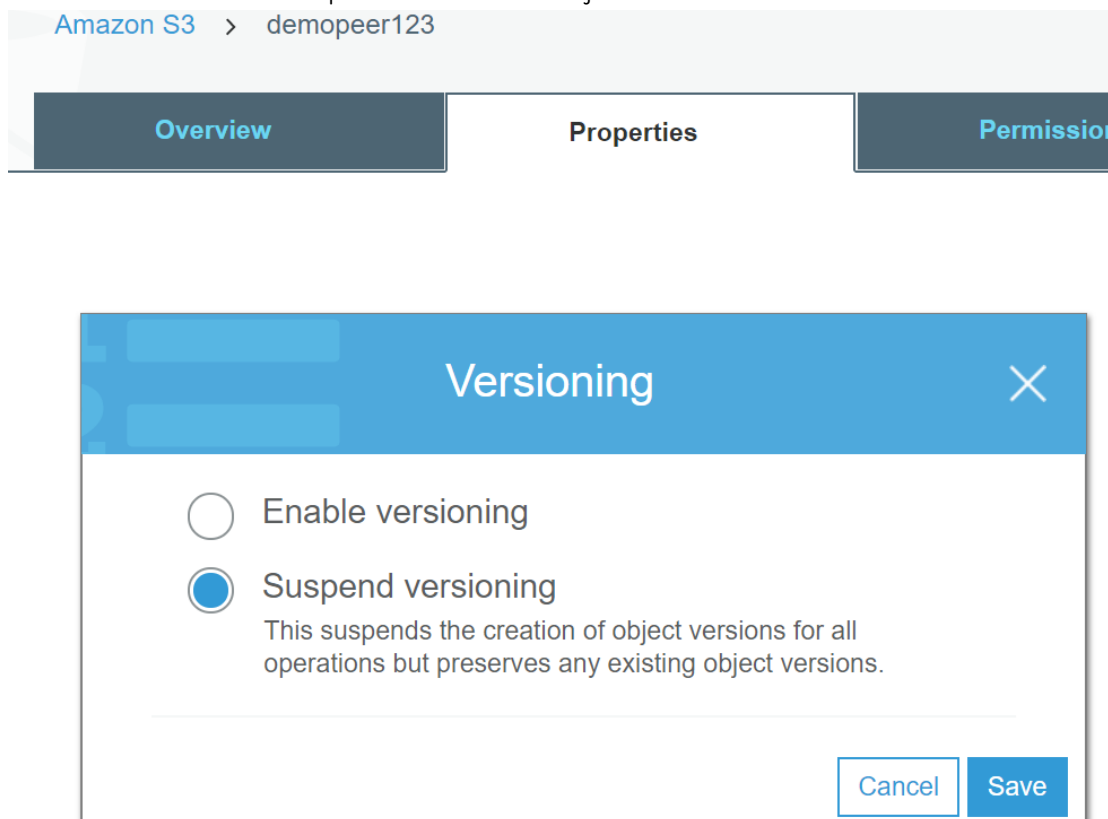
There is a requirement to store documents in AWS and the documents need to be version controlled. Which of the following storage options would be an ideal choice for this scenario?

- ☒ A. Amazon S3 ✓
- ☐ B. Amazon EBS
- ☐ C. Amazon EFS
- ☐ D. Amazon Glacier

#### Explanation :

##### Answer - A

Amazon S3 is a perfect storage layer for storing documents and other types of objects. Amazon S3 also has an option for versioning as shown below. Here, versioning is on the bucket level and can be used to recover prior versions of an object.



For more information on Amazon S3, please visit the following URL:  
<https://aws.amazon.com/s3/> (<https://aws.amazon.com/s3/>)

Ask our Experts



QUESTION 2

CORRECT

DESIGN RESILIENT ARCHITECTURES

An application currently consists of an EC2 Instance hosting a Web application. The Web application connects to an AWS RDS database. Which of the following can be used to ensure that the database layer is highly available?

- ☐ A. Create another EC2 Instance in another Availability Zone and host a replica of the database.
- ☐ B. Create another EC2 Instance in another Availability Zone and host a replica of the Webserver.
- ☐ C. Enable Read Replica for the AWS RDS database.
- ☒ D. Enable Multi-AZ for the AWS RDS database. ✓

#### Explanation :

##### Answer – D

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. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

For more information on AWS RDS Multi-AZ, please visit the following URL:

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

Ask our Experts



QUESTION 3

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

An application currently accepts users to upload files to an S3 bucket. You want to ensure that the file name for each uploaded file is stored in a DynamoDB table. How can this be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution.

- ☒ A. Create an AWS Lambda function to insert the required entry for each uploaded file. ✓
- ☐ B. Use AWS CloudWatch to probe for any S3 event.
- ☒ C. Add an event with notification send to Lambda. ✓
- ☐ D. Add the CloudWatch event to the DynamoDB table streams section.

**Explanation :**

**Answer – A and C**

You can create a Lambda function containing the code to process the file, and add the name of the file to the DynamoDB table.

You can then use an Event Notification from the S3 bucket to invoke the Lambda function whenever the file is uploaded.

# Events ×

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

Name	Events	Filter	Type
New event <span>×</span>			

Name i

*e.g. MyEmailEventForPut*

Events i

- |  |  |
|--|--|
| <input type="checkbox"/> RRSObjectLost             | <input type="checkbox"/> Delete                |
| <input type="checkbox"/> Put                       | <input type="checkbox"/> Delete Marker Created |
| <input type="checkbox"/> Post                      | <input type="checkbox"/> ObjectCreate (All)    |
| <input type="checkbox"/> Copy                      | <input type="checkbox"/> ObjectDelete (All)    |
| <input type="checkbox"/> Complete Multipart Upload |  |

For more information on Amazon S3 Event Notifications, please visit the following URL:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>  
(<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html>)

Ask our Experts



A company is migrating an on-premises MySQL database to AWS.

Following are the key requirements:

- a) Ability to support an initial size of 5TB
- b) Ability to allow the database to double in size
- c) Replication Lag to be kept under 100 milliseconds

Which Amazon RDS engine meets these requirements?

- ☐ A. MySQL
- ☐ B. Microsoft SQL Server
- ☐ C. Oracle
- ☒ D. Amazon Aurora ✓

**Explanation :**

**Answer – D**

The AWS Documentation explains about how AWS Aurora fulfills the mentioned requirements: Amazon Aurora (Aurora) is a fully managed, MySQL- and PostgreSQL-compatible, relational database engine. It combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

All Aurora Replicas return the same data for query results with minimal replica lag—usually much lesser than 100 milliseconds after the primary instance has written an update.

For more information on AWS Aurora, please visit the following URL:

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Overview.html>  
(<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Overview.html>)

Ask our Experts



QUESTION 5

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

A company is required to host a static web site in AWS. Which of the following would be an easy and cost-effective way to set this up?

- ☐ A. Use CloudFormation templates to have the web site setup.
- ☐ B. Create an EC2 Instance , install the web server and then have the site setup.
- ☒ C. Use S3 web site hosting to host the web site. ✓
- ☐ D. Use Elastic Beanstalk to host the web site.

**Explanation :**

**Answer – C**

AWS Documentation mentions the following:

You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts.

For more information on AWS S3 web site hosting, please visit the following URL:

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

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>)

Ask our Experts



QUESTION 6

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

An application needs to have a database hosted in AWS. The database will be hosted on an EC2 Instance. The application itself does not have a high usage ratio, hence the reads and writes on the database would be limited to a bare minimum. What is the MOST suitable storage type that could be used by the underlying EC2 instance hosting the database?

- ☐ A. Amazon EBS provisioned IOPS SSD
- ☐ B. Amazon EBS Throughput Optimized HDD
- ☒ C. Amazon EBS General Purpose SSD ✓
- ☐ D. Amazon EFS

#### Explanation :

##### Answer - C

AWS recommends that for small workloads it is better to use General Purpose SSD volume (gp2) than Throughput Optimized HDD volumes.(st1).

As per the AWS docs :

##### Throughput Optimized HDD (st1) Volumes

Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported.

Throughput Optimized HDD (st1) volumes, though similar to Cold HDD (sc1) volumes, are designed to support frequently accessed data.

Note:

This volume type is optimized for workloads involving large, sequential I/O, and we recommend that customers with workloads performing small, random I/O use gp2. For more information, see Inefficiency of Small Read/Writes on HDD.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#inefficiency>  
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#inefficiency>)

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as you add and remove files, so your applications have the storage they need, when they need it. The service is designed to be highly scalable, highly available, and highly durable. Amazon EFS file systems store data and metadata across multiple Availability Zones in a region and can grow to petabyte scale, drive high levels of throughput, and allow massively parallel access from Amazon EC2 instances to your data.



In question they mentioned that "The application itself does not have a high usage ratio, hence the reads and writes on the database would be limited to a bare minimum". Ability to Reads & Writes of an application depends on IOPS ratio.

Since the database is not going to be used that frequently, you should ideally choose the EBS General Purpose SSD over EBS provisioned IOPS SSD.

For more information on AWS EBS Volumes, please visit the following URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>  
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>)

Ask our Experts



QUESTION 7

CORRECT

DEFINE PERFORMANT ARCHITECTURES

An application needs to have files stored in AWS. The file system needs to have the ability to be mounted on various Linux EC2 Instances. Which of the following would be an ideal storage service for this requirement?

- ☐ A. Amazon EBS
- ☒ B. Amazon EFS ✓
- ☐ C. Amazon S3
- ☐ D. Amazon EC2 Instance store

Explanation :

**Answer – B**

AWS Documentation mentions the following:

Amazon EFS provides scalable file storage for use with Amazon EC2. You can create an EFS file system and configure your instances to mount the file system. You can use an EFS file system as a common data source for workloads and applications running on multiple instances.

For more information on AWS EFS, please visit the following URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html>  
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html>)

Ask our Experts



QUESTION 8

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

An application allows users to upload images to an S3 bucket. Initially these images will be downloaded quite frequently, but after some time, the images might only be accessed once a week and the retrieval time should be as minimal as possible.

What could be done to ensure a COST effective solution? Choose 2 answers from the options below. Each answer forms part of the solution.

- ☐ A. Store the objects in Amazon Glacier.
- ☒ B. Store the objects in S3 – Standard storage. ✓
- ☐ C. Create a Lifecycle Policy to transfer the objects to S3 – Standard storage after a certain duration of time.
- ☒ D. Create a Lifecycle Policy to transfer the objects to S3 – Infrequent Access storage after a certain duration of time. ✓

**Explanation :**

**Answer – B and D**

Store the images initially in Standard storage since they are accessed frequently. Define Lifecycle Policies to move the images to Infrequent Access storage to save on costs.

Amazon S3 Infrequent access is perfect if you want to store data that is not frequently accessed, and is much more cost-effective than Option C i.e. Amazon S3 Standard. Also, if you choose Amazon Glacier with expedited retrievals, you defeat the whole purpose of the requirement, because this option would result in increased costs.

For more information on AWS Storage classes, please visit the following URL:

<https://aws.amazon.com/s3/storage-classes/> (<https://aws.amazon.com/s3/storage-classes/>)

Ask our Experts



QUESTION 9

CORRECT

DESIGN RESILIENT ARCHITECTURES

A company needs a solution to store and archive corporate documents and has determined that Amazon Glacier is the right solution. It is required that data is delivered within 5 minutes of a retrieval request.

Which feature in Amazon Glacier can help meet this requirement?

- ☐ A. Defining a Vault Lock
- ☒ B. Using Expedited retrieval ✓
- ☐ C. Using Bulk retrieval
- ☐ D. Using Standard retrieval

**Explanation :**

**Answer – B**

The AWS Documentation mentions the following:

Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required.

For more information on AWS Glacier Retrieval, please visit the following URL:

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html>  
(<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html>)

Ask our Experts



QUESTION 10

MARKED AS REVIEW

CORRECT

DEFINE PERFORMANT ARCHITECTURES

A company wants to use Kubernetes as an orchestration tool for their application containers. They need to have a fully managed solution for this. Which one of the following services would help fulfill this requirement?

- ☒ A. AWSEKS ✓
- ☐ B. AWS Lambda
- ☐ C. AWS API Gateway
- ☐ D. AWSELB

Explanation :

**Answer - A**

AWS Documentation mentions the following:

Amazon Elastic Container Service for Kubernetes (Amazon EKS) is a managed service that makes it easy for you to run Kubernetes on AWS without needing to install and operate your own Kubernetes clusters.

For more information on AWS Elastic Container service for Kubernetes, please visit the following URL:

<https://aws.amazon.com/eks/> (<https://aws.amazon.com/eks/>)

Ask our Experts



QUESTION 11

CORRECT

DEFINE PERFORMANT ARCHITECTURES

You plan to use Auto Scaling groups to maintain the performance of your web application. How can you ensure that the scaling activity has sufficient time to stabilize without executing another scaling action?

- ☐ A. Modify the Instance User Data property with a timeout interval.
- ☒ B. Increase the Auto Scaling Cooldown timer value. ✓
- ☐ C. Enable the Auto Scaling cross zone balancing feature.
- ☐ D. Disable CloudWatch alarms till the application stabilizes.

**Explanation :**

**Answer – B**

AWS Documentation mentions the following:

The Cooldown period is a configurable setting for your Auto Scaling group which ensures that it doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple Scaling Policy, it waits for the Cooldown period to complete before resuming scaling activities.

For more information on Auto Scaling Cooldown, please visit the following URL:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/Cooldown.html>  
(<https://docs.aws.amazon.com/autoscaling/ec2/userguide/Cooldown.html>)

Ask our Experts



QUESTION 12

CORRECT

SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet created with default ACL settings. The IT Security department has identified a DoS attack from a suspecting IP. How can you protect the subnets from this attack?

- ☐ A. Change the Inbound Security Groups to deny access from the suspecting IP.

- ☐ B. Change the Outbound Security Groups to deny access from the suspecting IP.
- ☒ C. Change the Inbound NACL to deny access from the suspecting IP. ✓
- ☐ D. Change the Outbound NACL to deny access from the suspecting IP.

**Explanation :**

**Answer – C**

Option A and B are invalid because the Security Groups already block traffic by default. You can use NACL's as an additional security layer for the subnet to deny traffic.

Option D is invalid since just changing the Inbound Rules is sufficient.

AWS Documentation mentions the following:

A Network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

For more information on Network Access Control Lists, please visit the following URL:

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

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

Ask our Experts



QUESTION 13

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company is planning on allowing their users to upload and read objects from an S3 bucket. Due to the numerous amount of users, the read/write traffic will be very high. How should the architect maximize Amazon S3 performance?

- ☒ A. Prefix each object name with a random string. ✓
- ☐ B. Use the STANDARD\_IA storage class.
- ☐ C. Prefix each object name with the current data.
- ☐ D. Enable versioning on the S3 bucket.

### Explanation :

#### Answer – A

If the request rate is high, you can use hash keys or random strings to prefix to the object name. Here, partitions used to store the objects will be better distributed and hence allow for better read/write performance for your objects.

For more information on how to ensure performance in S3, please visit the following URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html>)

Ask our Experts



QUESTION 14

CORRECT

DEFINE PERFORMANT ARCHITECTURES

An EC2 Instance setup in AWS will host an application which will make API calls to the Simple Storage Service. What is an ideal way for the application to access the Simple Storage Service?

- ☐ A. Pass API credentials to the instance using instance user data.
- ☐ B. Store API credentials as an object in a separate Amazon S3 bucket.
- ☐ C. Embed the API credentials into your application.
- ☒ D. Create and Assign an IAM role to the EC2 Instance. ✓

### Explanation :

#### Answer - D

AWS Documentation mentions the following:

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. It is not a good practice to use IAM credentials for a production-based application. It is always a good practice to use IAM Roles.

For more information on IAM Roles, please visit the following URL:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

([https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html))

Ask our Experts



QUESTION 15

CORRECT

DEFINE PERFORMANT ARCHITECTURES

Videos are uploaded to an S3 bucket, and you need to provide access to users to view the same. What is the best way to do so, while maintaining a good user experience for all users regardless of the region in which they are located?

- ☐ A. Enable Cross-Region Replication for the S3 bucket to all regions.
- ☒ B. Use CloudFront with the S3 bucket as the source. ✓
- ☐ C. Use API Gateway with S3 bucket as the source.
- ☐ D. Use AWS Lambda functions to deliver the content to users.

**Explanation :**

**Answer – B**

AWS Documentation mentions the following to backup this requirement:

Amazon CloudFront is a web service that speeds up distribution of static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called Edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the Edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance. If the content is already in the Edge location with the lowest latency, CloudFront delivers it immediately. If the content is not in that Edge location, CloudFront retrieves it from an Amazon S3 bucket or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

For more information on Amazon CloudFront, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>  
(<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>)



Ask our Experts



QUESTION 16

CORRECT

DESIGN RESILIENT ARCHITECTURES

An organization has a requirement to store 10TB worth of scanned files. They are required to have a search application in place to search through the scanned files.

Which of the below mentioned options is ideal for implementing the search facility?

- ☐ A. Use S3 with reduced redundancy to store and serve the scanned files. Install a commercial search application on EC2 Instances and configure with Auto-Scaling and an ElasticLoad Balancer.
- ☐ B. Model the environment using CloudFormation. Use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the scanned files with a search index.
- ☒ C. Use S3 with standard redundancy to store and serve the scanned files. Use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple Availability Zones. ✓
- ☐ D. Use a single-AZ RDS MySQL instance to store the search index for the scanned files and use an EC2 instance with a custom application to search based on the index.

**Explanation :**

**Answer – C**

With Amazon CloudSearch, you can quickly add rich search capabilities to your website or application. You don't need to become a search expert or worry about hardware provisioning, setup, and maintenance. With a few clicks in the AWS Management Console, you can create a search domain and upload the data that you want to make searchable, and Amazon CloudSearch will automatically provision the required resources and deploy a highly tuned search index.

You can easily change your search parameters, fine tune search relevance, and apply new settings at any time. As your volume of data and traffic fluctuates, Amazon CloudSearch seamlessly scales to meet your needs.

For more information on AWS CloudSearch , please visit the below link:

<https://aws.amazon.com/cloudsearch/> (<https://aws.amazon.com/cloudsearch/>)

Ask our Experts



QUESTION 17

CORRECT

DEFINE PERFORMANT ARCHITECTURES

You work as an AWS Architect for a company which has an on-premises data center. They want to connect their on-premises infra to the AWS Cloud. How can this be achieved?

Note that this connection must have the maximum throughput and be dedicated for the company.

- ☐ A. Use AWS Express Route
- ☒ B. Use AWS Direct Connect ✓
- ☐ C. Use AWS VPC Peering
- ☐ D. Use AWS VPN

**Explanation :**

**Answer - B**

AWS Documentation mentions the following:

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

For more information on AWS Direct Connect, please visit the below link:

<https://aws.amazon.com/directconnect/> (<https://aws.amazon.com/directconnect/>)

Ask our Experts



QUESTION 18

CORRECT

DESIGN RESILIENT ARCHITECTURES

A concern raised in your company is that developers could potentially delete production-based EC2 resources. As a Cloud Admin, which of the below options would you choose to help alleviate this concern? Choose 2 options.

- ☒ **A.** Tag the production instances with a production-identifying tag and add resource-level permissions to the developers with an explicit deny on the terminate API call to instances with the production tag. ✓
- ☒ **B.** Create a separate AWS account and add the developers to that account. ✓
- ☐ **C.** Modify the IAM policy on the developers to require MFA before deleting EC2 instances, and disable MFA access to the employee.
- ☐ **D.** Modify the IAM policy on the developers to require MFA before deleting EC2 instances.

#### Explanation :

##### Answer – A and B

Creating separate AWS account for developers will help the organization to facilitate the highest level of resource and security isolation.

The following documentation from AWS gives us a clear picture of the scenarios when we need to consider creating multiple accounts.

##### When to Create Multiple Accounts

While there is no one-size-fits-all answer for how many AWS accounts a particular customer should have, most companies will want to create more than one AWS account because multiple accounts provide the highest level of resource and security isolation. Answering “yes” to any of the following questions is a good indication that you should consider creating additional AWS accounts:

- *Does the business require administrative isolation between workloads?*

Administrative isolation by account provides the most straightforward approach for granting independent administrative groups different levels of administrative control over AWS resources based on the workload, development lifecycle, business unit (BU), or data sensitivity.

- *Does the business require limited visibility and discoverability of workloads?*

Accounts provide a natural boundary for visibility and discoverability. Workloads cannot be accessed or viewed unless an administrator of the account enables access to users managed in another account.

- *Does the business require isolation to minimize the blast radius?*

Blast-radius isolation by account provides a mechanism for limiting the impact of a critical event such as a security breach, if an AWS Region or Availability Zone becomes unavailable, account suspensions, etc. Separate accounts help define boundaries and provide natural blast-radius isolation.

- *Does the business require strong isolation of recovery and/or auditing data?*

Businesses that are required to control access and visibility to auditing data due to regulatory requirements can isolate their recovery data and/or auditing data in an account separate from where they run their workloads (e.g., writing CloudTrail logs to a different account).

For more information:

<https://aws.amazon.com/answers/account-management/aws-multi-account-security-strategy/>  
(<https://aws.amazon.com/answers/account-management/aws-multi-account-security-strategy/>)

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type – you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define.

For more information on tagging AWS resources, please refer to the below URL:

[http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)  
([http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html))

The question says that the developers should not have the option to delete production based resources. So, option A and B completely keep the developers away from production resources.

You wish to use MFA, which means developers can delete the production-based resources if they know MFA code which is not recommended.

AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

Organizations have good control on newly created accounts rather than old aws accounts. Because they can easily monitor and maintain(few) assigned permissions on accounts and they delete those accounts once the required task will be done.

Ask our Experts



QUESTION 19

CORRECT

DESIGN RESILIENT ARCHITECTURES

A company needs to monitor the read and write IOPS metrics for their AWS MySQL RDS instance and send real-time alerts to their Operations team. Which AWS services can accomplish this? Choose 2 answers from the options given below.

- ☐ A. Amazon Simple Email Service
- ☒ B. Amazon CloudWatch ✓
- ☐ C. Amazon Simple Queue Service
- ☐ D. Amazon Route 53
- ☒ E. Amazon Simple Notification Service ✓

Explanation :

**Answer – B and E**

Amazon CloudWatch may be used to monitor IOPS metrics from the RDS instance and Amazon Simple Notification Service, to send the notification if any alarm is triggered.

For more information on CloudWatch metrics, please refer to the link below.

[http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW\\_Support\\_For\\_AWS.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html)

([http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW\\_Support\\_For\\_AWS.html](http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html))

Ask our Experts



QUESTION 20

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You run an ad-supported photo-sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to photos on your site, causing loss to your business. What is an effective method to mitigate this? Choose the correct answer from the options below:

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

#### Explanation :

##### Answer – C

You can distribute private content using a signed URL that is valid for only a short time—possibly for as little as a few minutes. Signed URLs that are valid for such a short period are good for distributing content on-the-fly to a user for a limited purpose, such as distributing movie rentals or music downloads to customers on demand.

For more information on Signed URLs please visit the below link:

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>  
(<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>)

Ask our Experts



QUESTION 21

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company wants to setup a template for deploying resources to AWS. They want this to be dynamic in nature so that the template can pick up parameters and then spin up resources based on those parameters. Which of the following AWS services would be ideal for this requirement?

- ☐ A. AWS Beanstalk

- ☒ B. AWS CloudFormation ✓
- ☐ C. AWS CodeBuild
- ☐ D. AWS CodeDeploy

**Explanation :**

**Answer - B**

The AWS Documentation mentions the below on AWS CloudFormation. This supplements the requirement in the question about consultants using their architecture diagrams to construct CloudFormation templates.

AWS CloudFormation is a service that helps you model and set up your Amazon Web Service 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.

For more information on AWS CloudFormation, please visit the following URL:

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

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html>)

Ask our Experts



QUESTION 22

CORRECT

SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances needs to be encrypted. Which of the following can help achieve this?

- ☒ A. AWS KMS ✓
- ☐ B. AWS Certificate Manager
- ☐ C. API Gateway with STS
- ☐ D. IAM Access Key

### Explanation :

#### Answer – A

Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates used to encrypt traffic in transit, but not at rest.

Option C is incorrect - This is used for issuing tokens when using the API gateway for traffic in transit.

Option D is incorrect - This is used for secure access to EC2 Instances.

The AWS Documentation mentions the following on AWS KMS:

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage.

For more information on AWS KMS, please visit the following URL:

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

(<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>)

Ask our Experts



QUESTION 23

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

A company's business continuity department is worried about the EBS Volumes hosted in AWS and wants to ensure that redundancy is achieved for the same. What must be done to achieve this in a cost-effective manner?

- ☒ A. Nothing, since by default, EBS Volumes are replicated within their Availability Zones. ✓
- ☐ B. Copy the data to S3 bucket for data redundancy.
- ☐ C. Create EBS Snapshots in another Availability Zone for data redundancy.
- ☐ D. Copy the data to a DynamoDB table for data redundancy.



## Explanation :

### Answer – A

The AWS Documentation mentions the following:

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes offer the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes – all while paying a low price for only what you provision.

For more information on EBS, please visit the following URL:

<https://aws.amazon.com/ebs/> (<https://aws.amazon.com/ebs/>)

### Note:

Amazon EBS Availability & Durability:

Amazon EBS volumes are designed to be highly available and reliable. At no additional charge to you, Amazon EBS volume data is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component

Amazon EBS volumes are designed for an annual failure rate (AFR) of between 0.1% - 0.2%, where failure refers to a complete or partial loss of the volume, depending on the size and performance of the volume. This makes EBS volumes 20 times more reliable than typical commodity disk drives, which fail with an AFR of around 4%. For example, if you have 1,000 EBS volumes running for 1 year, you should expect 1 to 2 will have a failure. EBS also supports a snapshot feature, which is a good way to take point-in-time backups of your data.

Please refer below link.

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

(<https://aws.amazon.com/ebs/details/#AvailabilityandDurability>)

We need to notice two things. one - the question says that we need to achieve in a cost-effective manner. Two - we are testing whether you understood the core functionality of the service in CSAA exam. You can expect this kind of question in the AWS exam as well. Try to understand the question and answer.

In the exam, if they mentioned specifically about the replication based on the multi-AZ, then you can go with the Option C. So based on the question, the answer will differ.

Ask our Experts



A mobile application hosted on AWS needs to access a Data Store in AWS. With each item measuring around 10KB in size, the latency of data access must remain consistent despite very high application traffic. Which of the following would be an ideal Data Store for the application?

- ☒ A. AWS DynamoDB ✓
- ☐ B. AWS EBS Volumes
- ☐ C. AWS Glacier
- ☐ D. AWS Redshift

**Explanation :**

**Answer - A**

AWS Documentation mentions the following:

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity, makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

For more information on AWS DynamoDB, please visit the following URL:

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

Ask our Experts



A company is planning to design a Microservices architected application that will be hosted in AWS. This entire architecture needs to be decoupled whenever possible. Which of the following services can help achieve this? Please select 2 correct options.

- ☒ A. AWS SNS ✓
- ☐ B. AWS ELB
- ☐ C. AWS Auto Scaling
- ☒ D. AWS SQS ✓

**Explanation :**

**Answer – A and D**

AWS Documentation mentions the following:

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available.

- For more information on AWS SQS, please visit the following URL:
  - <https://aws.amazon.com/sqs/> (<https://aws.amazon.com/sqs/>)
- For more information on AWS SNS, please visit the following URL:
  - <https://aws.amazon.com/blogs/compute/implementing-enterprise-integration-patterns-with-aws-messaging-services-point-to-point-channels/>  
(<https://aws.amazon.com/blogs/compute/implementing-enterprise-integration-patterns-with-aws-messaging-services-point-to-point-channels/>)

Ask our Experts



You are developing a mobile application that needs to issue temporary security credentials to users. This is essential due to security concerns. Which of the below services can help achieve this?

- ☒ A. AWS STS ✓
- ☐ B. AWS Config
- ☐ C. AWS Trusted Advisor
- ☐ D. AWS Inspector

**Explanation :**

**Answer - A**

AWS Documentation mentions the following:

You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials are *short-term*, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them.

For more information on the Secure Token Service, please visit the following URL:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_temp.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

([https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_temp.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html))

Ask our Experts



QUESTION 27

MARKED AS REVIEW

CORRECT

DEFINE PERFORMANT ARCHITECTURES

Your architecture for an application currently consists of EC2 Instances sitting behind a classic ELB. The EC2 Instances are used to serve an application and are accessible through the internet. What can be done to improve this architecture in the event that the number of users accessing the application increases?

- ☐ A. Add another ELB to the architecture.
- ☒ B. Use Auto Scaling Groups. ✓
- ☐ C. Use an Application Load Balancer instead.
- ☐ D. Use the Elastic Container Service.

**Explanation :**

**Answer – B**

AWS Documentation mentions the following:

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it is easy to setup application scaling for multiple resources across multiple services in minutes.

For more information on AWS Auto Scaling, please visit the following URL:

<https://aws.amazon.com/autoscaling/> (<https://aws.amazon.com/autoscaling/>)

Ask our Experts



QUESTION 28

CORRECT

DEFINE PERFORMANT ARCHITECTURES

You are an architect for a gaming application which is in the design phase. Which of the following services can be used to ensure optimal performance and least latency for gaming users?

- ☐ A. AWS Auto Scaling
- ☐ B. AWS ELB
- ☒ C. AWS ElastiCache ✓
- ☐ D. AWS VPC

**Explanation :**

### Answer - C

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. Amazon ElastiCache is a popular choice for Gaming, Ad-Tech, Financial Services, Healthcare, and IoT apps.

For more information on AWS ElastiCache, please visit the following URL:

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

Ask our Experts



QUESTION 29

CORRECT

DEFINE PERFORMANT ARCHITECTURES

You are the architect for a business intelligence application which reads data from a MySQL database hosted on an EC2 Instance. The application experiences a high number of read and write requests.

Which Amazon EBS Volume type can meet the performance requirements of this database?

- ☒ A. EBS Provisioned IOPS SSD ✓
- ☐ B. EBS Throughput Optimized HDD
- ☐ C. EBS General Purpose SSD
- ☐ D. EBS Cold HDD

### Explanation :

#### Answer – A

Since there is a high performance requirement with high IOPS needed, one needs to opt for EBS Provisioned IOPS SSD.

The below snapshot from AWS Documentation mentions the need for using Provisioned IOPS for better IOPS performance for database-based applications.

Solid-State Drives (SSD)		
General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	TI H
General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Lo di a in
<ul style="list-style-type: none"> <li>• Recommended for most workloads</li> <li>• System boot volumes</li> <li>• Virtual desktops</li> <li>• Low-latency interactive apps</li> <li>• Development and test environments</li> </ul>	<ul style="list-style-type: none"> <li>• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume</li> <li>• Large database workloads, such as: <ul style="list-style-type: none"> <li>◦ MongoDB</li> <li>◦ Cassandra</li> <li>◦ Microsoft SQL Server</li> <li>◦ MySQL</li> <li>◦ PostgreSQL</li> <li>◦ Oracle</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>•</li> <li>•</li> <li>•</li> <li>•</li> </ul>

For more information on AWS EBS Volume types, please visit the following URL:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

Ask our Experts



An organization planning to use AWS for their production roll out, wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3 and setup the ELB. Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?

- ☒ A. AWS Elastic Beanstalk ✓
- ☐ B. AWS CloudFront
- ☐ C. AWS CloudFormation
- ☐ D. AWS DevOps

#### Explanation :

##### Answer – A

The Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services.

We can simply upload code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, Auto-Scaling, to application health monitoring. Meanwhile, we can retain full control over the AWS resources used in the application and access the underlying resources at any time.

Hence, A is the CORRECT answer.

For more information on launching a LAMP stack with Elastic Beanstalk, follow the below link.

<https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/>

(<https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/>)

##### How is AWS CloudFormation different from AWS Elastic Beanstalk?

These services are designed to complement each other. AWS Elastic Beanstalk (<https://aws.amazon.com/elasticbeanstalk/>) provides an environment to easily deploy and run applications in the cloud. It is integrated with developer tools and provides a one-stop experience for you to manage the lifecycle of your applications. AWS CloudFormation is a convenient provisioning mechanism for a broad range of AWS resources (<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-supported-resources.html>). It supports the infrastructure needs of many different types of applications such as existing enterprise applications, legacy applications, applications built using a variety of AWS



resources and container-based solutions (including those built using AWS Elastic Beanstalk).

Elastic BeanStalk as a Platform where I deploy an application. Cloudformation is "where I define a stack of resources".

Elastic BeanStalk is good for the relatively narrow use case of PaaS applications. and Cloudformation is good for the relatively broad use of defining Infrastructure as Code.

In question they asked about " Which of the below mentioned AWS services meets the requirement for making an orderly deployment of the software?". We are not provisioning broad range of AWS resources here.

So, Elastic Beanstalk will be a suitable answer.

Ask our Experts



QUESTION 31

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Your company is planning on using the API Gateway service to manage APIs for developers and users. There is a need to segregate the access rights for both developers and users. How can this be accomplished?

- ☒ A. Use IAM permissions to control the access. ✓
- ☐ B. Use AWS Access keys to manage the access.
- ☐ C. Use AWS KMS service to manage the access.
- ☐ D. Use AWS Config Service to control the access.

Explanation :

Answer - A

AWS Documentation mentions the following:

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

- To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
- To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

For more information on permissions for the API gateway, please visit the URL:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html>

(<https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html>)

Ask our Experts



QUESTION 32

CORRECT

DESIGN RESILIENT ARCHITECTURES

You currently have 2 development environments hosted in 2 different VPCs in an AWS account in the same region. There is now a need for resources from one VPC to access another. How can this be accomplished?

- ☐ A. Establish a Direct Connect connection.
- ☐ B. Establish a VPN connection.
- ☒ C. Establish VPC Peering. ✓
- ☐ D. Establish Subnet Peering.

Explanation :

**Answer – C**

AWS Documentation mentions the following:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. 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, with a VPC in another AWS account, or with a VPC in a different AWS Region.

For more information on VPC peering, please visit the URL:

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>  
(<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>)

Ask our Experts



QUESTION 33

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

Your company is planning on using the EMR service available in AWS for running their big data framework and wants to minimize the cost for running the EMR service. Which of the following could help achieve this?

- ☐ A. Running the EMR cluster in a dedicated VPC
- ☒ B. Choosing Spot Instances for the underlying nodes ✓
- ☐ C. Choosing On-Demand Instances for the underlying nodes
- ☐ D. Disable automated backups

#### Explanation :

##### Answer - B

AWS Documentation mentions the following:

Spot Instances in Amazon EMR provide an option to purchase Amazon EC2 instance capacity at a reduced cost as compared to On-Demand purchasing.

For more information on Instance types for EMR, please visit the URL:

- <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-instance-purchasing-options.html> (<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-instance-purchasing-options.html>)
- <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html> (<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html>)

Ask our Experts



QUESTION 34

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You have an S3 bucket hosted in AWS which is used to store promotional videos you upload. You need to provide access to users for a limited duration of time. How can this be achieved?

- ☐ A. Use versioning and enable a timestamp for each version.
- ☒ B. Use Pre-Signed URLs. ✓
- ☐ C. Use IAM Roles with a timestamp to limit the access.
- ☐ D. Use IAM policies with a timestamp to limit the access.

**Explanation :**

**Answer - B**

AWS Documentation mentions the following:

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

For more information on pre-signed URLs, please visit the URL below.

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

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>)

Ask our Experts



QUESTION 35

CORRECT

DESIGN RESILIENT ARCHITECTURES

An application currently writes a large number of records to a DynamoDB table in one region. There is a requirement for a secondary application to retrieve new records written to the DynamoDB table every 2 hours and process the updates accordingly. Which of the following is an ideal way to ensure that the secondary application gets the relevant changes from the DynamoDB table?

- ☐ A. Insert a timestamp for each record and then scan the entire table for the timestamp as per the last 2 hours.
- ☐ B. Create another DynamoDB table with the records modified in the last 2 hours.
- ☒ C. Use DynamoDB Streams to monitor the changes in the DynamoDB table. ✓
- ☐ D. Transfer records to S3 which were modified in the last 2 hours.

#### Explanation :

##### Answer – C

AWS Documentation mentions the following:

A DynamoDB Stream is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

Whenever an application creates, updates, or deletes items in the table, DynamoDB Streams write a stream record with the primary key attribute(s) of the items that were modified. A stream record contains information about a data modification to a single item in a DynamoDB table. You can configure the stream so that the stream records capture additional information, such as the "before" and "after" images of modified items.

For more information on DynamoDB Streams, please visit the below URL.

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>  
(<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>)

Ask our Experts



Your company has recently started using AWS services for their daily operations. As a cloud administrator, which of the following services would you recommend using to have an insight on securing the infrastructure and for cost optimization?

- ☐ A. AWS Inspector
- ☒ B. AWS Trusted Advisor ✓
- ☐ C. AWS WAF
- ☐ D. AWS Config

**Explanation :**

**Answer – B**

AWS Documentation mentions the following on Trusted Advisor:

An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

For more information on the Trusted Advisor, please visit the below URL:

<https://aws.amazon.com/premiumsupport/trustedadvisor/>  
(<https://aws.amazon.com/premiumsupport/trustedadvisor/>)

Ask our Experts



QUESTION 37

CORRECT

SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your IT Security department has mandated that all traffic flowing in and out of EC2 instances needs to be monitored. Which of the below services can help achieve this?

- ☐ A. Trusted Advisor
- ☒ B. VPC Flow Logs ✓

- ☐ C. Use CloudWatch metrics
- ☐ D. Use CloudTrail

**Explanation :**

**Answer – B**

AWS Documentation mentions the following:

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.

For more information on VPC Flow Logs, please visit the following URL:

- <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>  
(<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html>)

**Note:**

The question asks to monitor all traffic flowing in and out of EC2 instances. Now you have to launch EC2 instance inside the VPC. As there is no other Option available. To monitor the navigation of IP traffic we use **VPC Flow Logs**.

Coming to question - why not CloudTrail? Before venturing into it, let's look into the types of log categories we have in AWS.

**1. AWS Infrastructure Logs** - AWS CloudTrail, Amazon VPC Flow Logs

**2. AWS Service Logs** - Amazon S3, AWS Elastic Load Balancing, Amazon CloudFront, AWS Lambda, AWS Elastic Beanstalk, etc.,

**3. Host Based Logs** - Messages, Security, NGINX/Apache/IIS, Windows Event Logs, Windows Performance Counters, etc.,

AWS CloudTrail: it is used for recording AWS API calls for your account like,

- who made the API call?
- when was the API call made?
- what was the API call?
- which resources were acted upon in the API call?
- where was the API calls made from and made to?

Ask our Experts



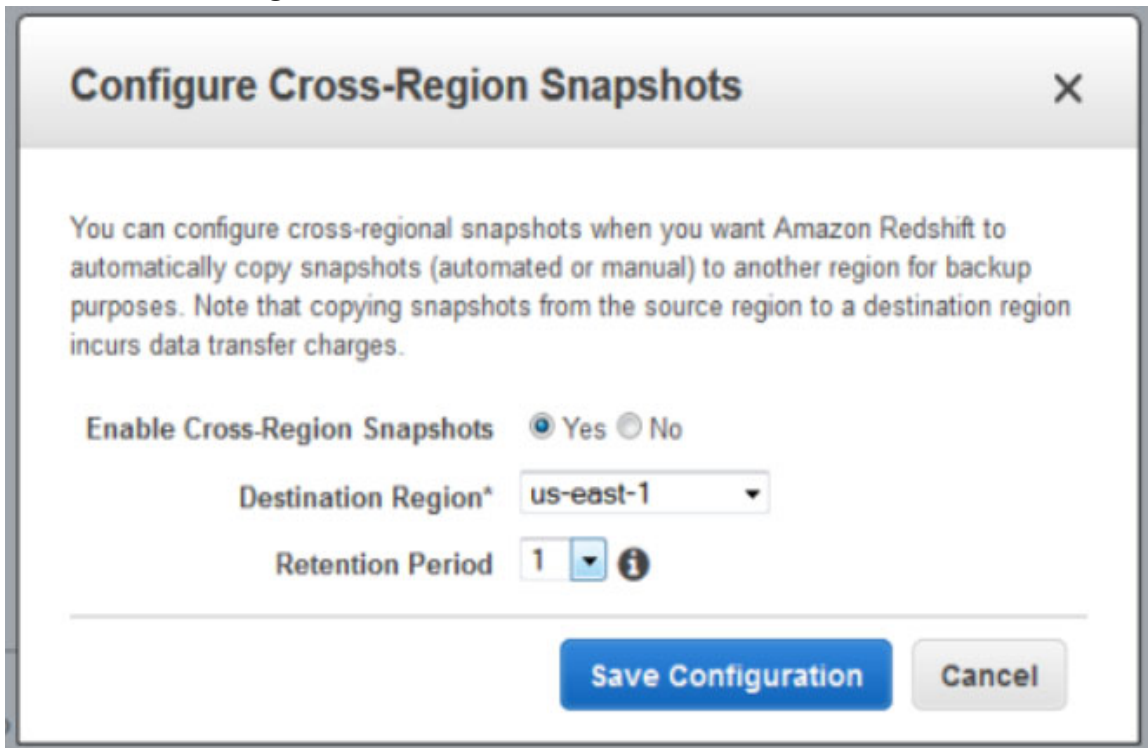
A company is currently utilising Redshift cluster as their production warehouse. As a cloud architect, you are tasked to ensure that the disaster recovery is in place. Which of the following options is best in addressing this issue?

- ☐ A. Take a copy of the underlying EBS volumes to S3 and then do Cross-Region Replication.
- ☒ B. Enable Cross-Region Snapshots for the Redshift Cluster. ✓
- ☐ C. Create a CloudFormation template to restore the Cluster in another region.
- ☐ D. Enable Cross Availability Zone Snapshots for the Redshift Cluster.

Explanation :

Answer – B

The below diagram shows that snapshots are available for Redshift clusters enabling them to be available in different regions:



**Configure Cross-Region Snapshots** [X]

You can configure cross-regional snapshots when you want Amazon Redshift to automatically copy snapshots (automated or manual) to another region for backup purposes. Note that copying snapshots from the source region to a destination region incurs data transfer charges.

Enable Cross-Region Snapshots ☒ Yes ☐ No

Destination Region\* us-east-1 ▼

Retention Period 1 ▼ ⓘ

Save Configuration Cancel

For more information on managing Redshift Snapshots, please visit the following URL:  
<https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html>



(<https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html>)

Ask our Experts



QUESTION 39

CORRECT

DESIGN RESILIENT ARCHITECTURES

You have an AWS RDS PostgreSQL database hosted in the Singapore region. You need to ensure that a backup database is in place and the data is asynchronously copied. Which of the following would help fulfill this requirement?

- ☐ A. Enable Multi-AZ for the database
- ☒ B. Enable Read Replicas for the database ✓
- ☐ C. Enable Asynchronous replication for the database
- ☐ D. Enable manual backups for the database

#### Explanation :

##### Answer – B

AWS Documentation mentions the following:

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

For more information on Read Replicas, please visit the following URL:

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

##### Note:

When you enable Multi-AZ for the database then we are enabling synchronous replication rather than asynchronous replication mentioned in the question.

When you create a Read Replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the **asynchronous replication** method for the DB engine to update the Read Replica whenever there is a change to the source DB instance.

You can use Read Replica promotion as a data recovery scheme if the source DB instance fails.

For more information please click the link given below:

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

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

Ask our Experts



QUESTION 40

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

Your current log analysis application takes more than four hours to generate a report of the top 10 users of your web application. You have been asked to implement a system that can report this information in real time, ensure that the report is always up to date, and handle increases in the number of requests to your web application. Choose the option that is cost-effective and can fulfill the requirements.

- ☐ A. Publish your data to CloudWatch Logs, and configure your application to Auto Scale to handle the load on demand.
- ☐ B. Publish your log data to an Amazon S3 bucket. Use AWS CloudFormation to create an Auto Scaling group to scale your post-processing application which is configured to pull down your log files stored in Amazon S3.

- ☒ C. Post your log data to an Amazon Kinesis data stream, and subscribe your log-processing application so that is configured to process your logging data. ✓
- ☐ D. Configure an Auto Scaling group to increase the size of your Amazon EMR cluster.

**Explanation :**

**Answer – C**

AWS Documentation mentions the below:

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as application logs, website clickstreams, IoT telemetry data, and more into your databases, data lakes and data warehouses, or build your own real-time applications using this data. Amazon Kinesis enables you to process and analyze data as it arrives and respond in real-time instead of having to wait until all your data is collected before the processing can begin.

For more information on AWS Kinesis, please see the below link:

<https://aws.amazon.com/kinesis/> (<https://aws.amazon.com/kinesis/>)

Ask our Experts



QUESTION 41

CORRECT

DEFINE PERFORMANT ARCHITECTURES

Your company wants to automate the deployment of new EC2 Instances. There is a need to have pre-baked Images so that the deployment of instances can be done in a faster manner. Which of the following options can help achieve this?

- ☐ A. Create an Elastic Beanstalk image.
- ☐ B. Create an OpsWorks image.
- ☒ C. Create an Amazon Machine image. ✓

☐ D. Create a Linux Container image.

**Explanation :**

**Answer – C**

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.

For more information on AMIs please see the below link:

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

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

Ask our Experts



QUESTION 42

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

There is a requirement to load a lot of data from your on-premises network on to AWS Redshift. Which of the below options can be used for this data transfer?

Choose 2 answers from the options given below.

- ☐ A. Data Pipeline
- ☒ B. Direct Connect ✓
- ☒ C. Snowball ✓
- ☐ D. AWS VPN

**Explanation :**

**Answer – B and C**

AWS documentation mentions the following about the above services:

With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premises data centers and Amazon Simple Storage Service (Amazon S3). AWS Snowball uses Snowball appliances and provides powerful interfaces that you can use to create jobs, transfer data, and track the status of your jobs through to completion. By shipping your data in Snowballs, you can transfer large amounts of data at a significantly faster rate than if you were transferring that data over the Internet, saving you time and money.

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1-gigabit or 10-gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create *virtual interfaces* directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing Internet service providers in your network path.

For more information on Direct Connect, please refer to the below URL:

<http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>  
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html>)

For more information on AWS Snowball, please refer to the below URL:

- <http://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>  
(<http://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>)

**Note:**

Virtual Private Networks designed for organizations where employees needed to connect to a certain computer from different locations without compromising security.

In the question they mentioned that ""There is a requirement to load a lot of data from your on-premises network on to AWS Redshift"". So, Direct connect will be the suitable option.

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

AWS Direct Connect makes it easy to scale your connection to meet your needs. AWS Direct Connect provides 1 Gbps and 10 Gbps connections, and you can easily provision multiple connections if you need more capacity.



QUESTION 43

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

Having created a Redshift cluster in AWS, you are trying to use SQL Client tools from an EC2 Instance, but aren't able to connect to the Redshift Cluster. What must you do to ensure that you are able to connect to the Redshift Cluster from the EC2 Instance?

- ☐ A. Install Redshift client tools on the EC2 Instance first.
- ☒ B. Modify the VPC Security Groups. ✓
- ☐ C. Use the AWS CLI instead of the Redshift client tools.
- ☐ D. Modify the NACL on the subnet.

**Explanation :**

**Answer – B**

AWS Documentation mentions the following:

By default, any cluster that you create is closed to everyone. IAM credentials only control access to the Amazon Redshift API-related resources: the Amazon Redshift console, command line interface (CLI), API, and SDK. To enable access to the cluster from SQL client tools via JDBC or ODBC, you use security groups:

- If you are using the EC2-Classical platform for your Amazon Redshift cluster, you must use Amazon Redshift security groups.
- If you are using the EC2-VPC platform for your Amazon Redshift cluster, you must use VPC security groups.

For more information on Amazon Redshift, please refer to the below URL:

<http://docs.aws.amazon.com/redshift/latest/mgmt/overview.html>

(<http://docs.aws.amazon.com/redshift/latest/mgmt/overview.html>)

Ask our Experts



QUESTION 44

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You currently work for a company that is specialised in baggage management. GPS devices installed on all the baggages, deliver the coordinates of the unit every 10 seconds. You need to process these coordinates in real-time from multiple sources. Which tool should you use to process the data?

- ☐ A. Amazon EMR
- ☐ B. Amazon SQS
- ☐ C. AWS Data Pipeline
- ☒ D. Amazon Kinesis ✓

**Explanation :**

**Answer – D**

The AWS Documentation mentions the following

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

For more information on Amazon Kinesis, please visit the link below.

<https://aws.amazon.com/kinesis/> (<https://aws.amazon.com/kinesis/>)

Ask our Experts



You are planning on hosting a web and MySQL database application in an AWS VPC. The database should only be accessible by the web server. Which of the following would you change to fulfill this requirement?

- ☐ A. Network Access Control Lists
- ☐ B. AWS RDS Parameter Groups
- ☐ C. Route Tables
- ☒ D. Security groups ✓

#### Explanation :

##### Answer – D

Security group associated with the db instance should allow port 3306 traffic from EC2 instance.

The AWS Documentation additionally 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.

For more information on VPC Security Groups, please visit the link below.

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

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

Ask our Experts





A company has a requirement for block level storage which would be able to store 800GB of data. Also, encryption of the data is required. Which of the following can be used in this case?

- ☒ A. AWS EBS Volumes ✓
- ☐ B. AWS S3
- ☐ C. AWS Glacier
- ☐ D. AWS EFS

**Explanation :**

**Answer - A**

For block level storage, consider EBS Volumes.

Options B and C are incorrect since they provide object level storage.

Option D is incorrect since this provides file level storage.

For more information on EBS Volumes, please visit the following URL:

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

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html>)

Ask our Experts



QUESTION 47

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

An application requires storage for an EC2 Instance for storing infrequently accessed data. Which of the following is a cost-effective, ideal storage option here?

- ☐ A. EBS IOPS
- ☐ B. EBS SSD

☐ C. EBS Throughput Optimized

☒ D. EBS Cold HDD ✓

### Explanation :

#### Answer – D

If you need storage for infrequently accessed data, then EBS Cold HDD is the best option.

This is also mentioned in the AWS Documentation:

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	<ul style="list-style-type: none"><li>• Recommended for most workloads</li><li>• System boot volumes</li><li>• Virtual desktops</li><li>• Low-latency interactive apps</li><li>• Development and test environments</li></ul>	<ul style="list-style-type: none"><li>• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume</li><li>• Large database workloads, such as:<ul style="list-style-type: none"><li>◦ MongoDB</li><li>◦ Cassandra</li><li>◦ Microsoft SQL Server</li><li>◦ MySQL</li><li>◦ PostgreSQL</li><li>◦ Oracle</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Streaming workloads requiring consistent, fast throughput at a low price</li><li>• Big data</li><li>• Data warehouses</li><li>• Log processing</li><li>• Cannot be a boot volume</li></ul>	<ul style="list-style-type: none"><li>• Throughput-oriented storage for large volumes of data that is infrequently accessed</li><li>• Scenarios where the lowest storage cost is important</li><li>• Cannot be a boot volume</li></ul>
API Name	gp2	io1	st1	sc1
Volume Size	1 GiB - 16 TiB	4 GiB - 16 TiB	500 GiB - 16 TiB	500 GiB - 16 TiB
Max. IOPS**/Volume	10,000	32,000	500	250
Max.	160 MiB/s	500 MiB/s***	500 MiB/s	250 MiB/s

For more information on EBS Volume types, please visit the following URL:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>  
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>)

Ask our Experts



QUESTION 48

CORRECT

DEFINE PERFORMANT ARCHITECTURES

As the cloud administrator of your company, you notice that one of EC2 instances is restarting frequently. There is a need to troubleshoot and analyse the system logs. What can be used in AWS to store and analyze the log files from the EC2 Instance? Choose one answer from the options below.

- ☐ A. AWS SQS
- ☐ B. AWS S3
- ☐ C. AWS CloudTrail
- ☒ D. AWS CloudWatch Logs ✓

**Explanation :**

**Answer – D**

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, and other sources.

For more information on CloudWatch Logs, please visit the following URL:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>  
(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>)

**Note:** The question is not about compliance or auditing or tracking any kind of malicious activity or to monitor api calls in your account. If that would have been the case we w'd have used cloudtrail as it provides info such as who made the request, when the request was made, What was the request, What was the response etc.

In this question we need cloudwatch logs to store and analyze logs from EC2 to find why the instance is restarting frequently.

Ask our Experts



QUESTION 49

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

Your company has migrated their production environment into AWS VPC 6 months ago. As a cloud architect, you are required to revise the infrastructure and ensure that it is cost-effective in the long term. There are more than 50 EC2 instances that are up and running all the time to support the business operation. What can you do to lower the cost?

- ☒ A. Reserved instances ✓
- ☐ B. On-demand instances
- ☐ C. Spot instances
- ☐ D. Regular instances

**Explanation :**

**Answer – A**

When you have instances that will be used continuously and throughout the year, the best option is to buy reserved instances. By buying reserved instances, you are actually allocated an instance for the entire year or the duration you specify with a reduced cost.

To understand more on reserved instances, please visit the below URL:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>  
(<https://aws.amazon.com/ec2/pricing/reserved-instances/>)

Ask our Experts



QUESTION 50

CORRECT

DESIGN RESILIENT ARCHITECTURES

Your organization is building a collaboration platform for which they chose AWS EC2 for web and application servers and MySQL RDS instance as the database. Due to the nature of the traffic to the application, they would like to increase the number of connections to RDS instance. How can this be achieved?

- ☐ A. Login to RDS instance and modify database config file under `/etc/mysql/my.cnf`
- ☒ B. Create a new parameter group, attach it to DB instance and change the setting.  
✓
- ☐ C. Create a new option group, attach it to DB instance and change the setting.
- ☐ D. Modify setting in default options group attached to DB instance.

**Explanation :**

**Answer – B**

You manage your DB engine configuration through the use of parameters in a DB parameter group . DB parameter groups act as a container for engine configuration values that are applied to one or more DB instances.

A default DB parameter group is created if you create a DB instance without specifying a customer-created DB parameter group. Each default DB parameter group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance. You cannot modify the parameter settings of a default DB parameter group; you must create your own DB parameter group to change parameter settings from their default value. Note that not all DB engine parameters can be changed in a customer-created DB parameter group.

**If you want to use your own DB parameter group, you simply create a new DB parameter group, modify the desired parameters, and modify your DB instance to use the new DB parameter group.** All DB instances that are associated with a particular DB parameter group get all parameter updates to that DB parameter group.

## Parameter Groups > mysqlcustom

Parameters						
Recent Events						
Tags						
Filter: Q conne X Cancel Editing Preview Changes Reset Parameters Save Changes						
Name	Edit Values	Allowed Values	Is Modifiable	Source	Apply Type	
back_log	<input type="text"/>	1-65535	true	engine-default	static	
character_set_connection	<engine-default>		true	engine-default	dynamic	
collation_connection	<engine-default>		true	engine-default	dynamic	
connect_timeout	<input type="text"/>	2-31536000	true	engine-default	dynamic	
init_connect	<input type="text"/>		true	engine-default	dynamic	
interactive_timeout	<input type="text"/>	1-31536000	true	engine-default	dynamic	
max_connect_errors	<input type="text"/>	1-18446744073709547520	true	engine-default	dynamic	
max_connections	[DBInstanceClassMemor	1-100000	true	system	dynamic	
max_user_connections	<input type="text"/>	0-4294967295	true	engine-default	dynamic	
net_read_timeout	<input type="text"/>	1-31536000	true	engine-default	dynamic	
net_write_timeout	<input type="text"/>	1-31536000	true	engine-default	dynamic	
performance_schema_session_connect_attrs_size	<input type="text"/>	-1-1048576	true	engine-default	static	
port	[EndPointPort]		false	system	static	
secure_auth	<engine-default>		true	engine-default	dynamic	
slave_net_timeout	<input type="text"/>	1-31536000	true	engine-default	dynamic	
socket	/tmp/mysql.sock		false	system	static	

For more information;

- [https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_WorkingWithParamGroups.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html)  
([https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_WorkingWithParamGroups.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html))

Ask our Experts



QUESTION 51

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

Your company needs to keep all system logs for audit purposes, and may rarely need to retrieve these logs for audit purposes and present them upon request within a week. The logs are 10TB in size. Which option would be the most cost-effective one for storing all these system logs?

- ☒ A. Amazon Glacier ✓
- ☐ B. S3-Reduced Redundancy Storage
- ☐ C. EBS backed storage connected to EC2
- ☐ D. AWS CloudFront

**Explanation :**

**Answer – A**

With the above requirements, the best option is to opt for Amazon Glacier.

AWS Documentation further mentions the following:

Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup. It is designed to deliver 99.999999999% durability, and provides comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.

For more information on Amazon Glacier, please refer to the below URL:

<https://aws.amazon.com/glacier/> (<https://aws.amazon.com/glacier/>)

Ask our Experts



QUESTION 52

CORRECT

DESIGN RESILIENT ARCHITECTURES

A company is building a service using Amazon EC2 as a worker instance that will process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. You do not know what the storage capacity requirements are. Which storage option is both cost-efficient and scalable?

- ☐ A. Multiple Amazon EBS Volume with snapshots
- ☐ B. A single Amazon Glacier vault
- ☒ C. A single Amazon S3 bucket ✓

☐ D. Multiple instance stores

**Explanation :**

**Answer – C**

Amazon S3 is the best storage option for this. It is durable and highly available.

For more information on Amazon S3, please refer to the below URL:

<https://aws.amazon.com/s3/> (<https://aws.amazon.com/s3/>)

Ask our Experts



QUESTION 53

MARKED AS REVIEW

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You have configured an Auto-scaling group for which the minimum running instance is 2 and maximum running instance is 10. For the past 30 minutes, all five instances have been running at 100 CPU Utilization; however, the Auto Scaling group has not added any more instances to the group. What is the most likely cause for this? Choose 2 answers from the options given below.

- ☒ A. You already have 20 on-demand instances running. ✓
- ☐ B. The Auto Scaling group's MAX size is set at five.
- ☐ C. The Auto Scaling group's scale down policy is too high.
- ☒ D. The Auto Scaling group's scale up policy has not yet been reached. ✓

**Explanation :**

**Answer – A and D**

By default, you can run up to 20 On-Demand EC2 instances. If you need more, you have to complete a requisition form and submit it to AWS.

However in the question, we have already mentioned that MAX is set to 10. In that case option B is



invalid and hence cannot be marked as an answer. But the question does not mention that the metric chosen for this Auto Scaling policy is CPUUtilization Metric. It could be DiskWrites or Network In/Out metric. Assuming the current set up is to do with a metric other than CPUUtilization we can choose option D as a right choice. In this scenario, we are only discussing about the non-functioning Scaling up process and not about the Scaling down scenario.

This is explained in the AWS documentation:

Depending on the instance types, some instance types only support up to 5 on-demand instances. However the maximum for most of the instance types are 20 on-demand instances. So based on that, Option A is correct.

**instance(s) are already running. Launching EC2 instance failed.**

**Cause:** The Auto Scaling group has reached the limit set by the DesiredCapacity parameter.

**Solution:** Update your Auto Scaling group by providing a new value for the --desired-capacity parameter using the update-auto-scaling-group command.

If you've reached your limit for the number of EC2 instances, you can request an increase. For more information, see AWS Service Limits.

For more information on troubleshooting Auto Scaling, please refer to the following link:

<http://docs.aws.amazon.com/autoscaling/latest/userguide/ts-as-capacity.html>

(<http://docs.aws.amazon.com/autoscaling/latest/userguide/ts-as-capacity.html>)

The link below provides information on EC2 instance limits:

[https://docs.aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html#limits\\_ec2](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2)

([https://docs.aws.amazon.com/general/latest/gr/aws\\_service\\_limits.html#limits\\_ec2](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2))

More information on limits of on-demand EC2 instances is available at:

[https://aws.amazon.com/ec2/faqs/#How\\_many\\_instances\\_can\\_I\\_run\\_in\\_Amazon\\_EC2](https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2)

([https://aws.amazon.com/ec2/faqs/#How\\_many\\_instances\\_can\\_I\\_run\\_in\\_Amazon\\_EC2](https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2))

Ask our Experts



QUESTION 54

CORRECT

DEFINE PERFORMANT ARCHITECTURES

Your company is utilising CloudFront to distribute its media content to multiple regions. The content is frequently accessed by users. As a cloud architect, which of the following options would help you improve the performance of the system?

☐ A. Change the origin location from an S3 bucket to an ELB.

- ☐ B. Use a faster Internet connection.
- ☒ C. Increase the cache expiration time. ✓
- ☐ D. Create an "invalidation" for all your objects, and recache them.

Explanation :

Answer – C

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin.

For more information on CloudFront cache expiration, please refer to the following link:

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>  
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>)

Ask our Experts



QUESTION 55

MARKED AS REVIEW

CORRECT

DESIGN RESILIENT ARCHITECTURES

You have been instructed by your supervisor to devise a disaster recovery model for the resources in their AWS account. The key requirement while devising the solution is to ensure that the cost is at a minimum. Which of the following disaster recovery mechanisms would you employ in such a scenario?

- ☒ A. Backup and Restore ✓
- ☐ B. Pilot Light
- ☐ C. Warm standby
- ☐ D. Multi-Site

### Explanation :

#### Answer – A

Since the cost needs to be at a minimum, the best option is to back up all the resources and then perform a restore in the event of a disaster.

For more information on disaster recovery, please refer to the below link:

[https://media.amazonwebservices.com/AWS\\_Disaster\\_Recovery.pdf](https://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf)

([https://media.amazonwebservices.com/AWS\\_Disaster\\_Recovery.pdf](https://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf))

Ask our Experts



QUESTION 56

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

An application consists of the following architecture:

- a. EC2 Instances are in multiple AZ's behind an ELB.
- b. The EC2 Instances are launched via an Auto Scaling Group.
- c. There is a NAT instance used so that instances can download updates from the internet.

Due to the high bandwidth being consumed by the NAT instance, it has been decided to use a NAT Gateway. How should this be implemented?

- ☐ A. Use NAT Instances along with the NAT Gateway.
- ☐ B. Host the NAT instance in the private subnet.

- ☒ C. Migrate the NAT Instance to NAT Gateway and host the NAT Gateway in the public subnet. ✓
- ☐ D. Convert the NAT instance to a NAT Gateway.

**Explanation :**

**Answer – C**

One can simply start using the NAT Gateway service and stop using the deployed NAT instances. But you need to ensure that the NAT Gateway is deployed in the public subnet.

For more information on migrating to a NAT Gateway, please visit the following URL:

<https://aws.amazon.com/premiumsupport/knowledge-center/migrate-nat-instance-gateway/>  
(<https://aws.amazon.com/premiumsupport/knowledge-center/migrate-nat-instance-gateway/>)

Ask our Experts



QUESTION 57

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

A company has an application hosted in AWS. This application consists of EC2 Instances that sit behind an ELB. The following are requirements from an administrative perspective:

- a) Must be able to collect and analyse logs with regard to ELB's performance.
- b) Ensure that notifications are sent when the latency goes beyond 10 seconds.

Which of the following can be used to achieve this requirement? Choose 2 answers from the options given below.

- ☒ A. Use CloudWatch for monitoring. ✓
- ☐ B. Enable CloudWatch logs and then investigate the logs whenever there is an issue.
- ☒ C. Enable the logs on the ELB with Latency Alarm that sends an email and then investigate the logs whenever there is an issue. ✓
- ☐ D. Use CloudTrail to monitor whatever metrics need to be monitored.

#### Explanation :

##### Answer – A and C

When you use CloudWatch metrics for an ELB, you can get the amount of read requests and latency out of the box.

For more information on using CloudWatch with the ELB, please visit the following URL:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-cloudwatch-metrics.html>  
(<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-cloudwatch-metrics.html>)

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.

For more information on using ELB logs, please visit the following URL:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html>  
(<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html>)

Ask our Experts



Your company would like to leverage the AWS storage option and integrate it with the current on-premises infrastructure. Additionally, due to business requirements, low latency access to all the data is a must. Which of the following options would be best suited for this scenario?

- ☐ A. Configure the Simple Storage Service.
- ☐ B. Configure Storage Gateway Cached Volume.
- ☒ C. Configure Storage Gateway Stored Volume. ✓
- ☐ D. Configure Amazon Glacier.

#### Explanation :

##### Answer – C

AWS Documentation mentions the following:

If you need low-latency access to your entire dataset, first configure your on-premises gateway to store all your data locally. Then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive offsite backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

For more information on the Storage Gateway, please visit the following URL:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>  
(<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>)

Ask our Experts



QUESTION 59

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

An IT company has a set of EC2 Instances hosted in a VPC. They are hosted in a private subnet. These instances now need to access resources stored in an S3 bucket. The traffic should not traverse the internet. The addition of which of the following would help fulfill this requirement?

- ☒ A. VPC Endpoint ✓
- ☐ B. NAT Instance
- ☐ C. NAT Gateway
- ☐ D. Internet Gateway

**Explanation :**

**Answer - A**

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

For more information on AWS VPC endpoints, please visit the following URL:

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

(<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>)

Ask our Experts



QUESTION 60

CORRECT

DESIGN RESILIENT ARCHITECTURES

You need to host a set of web servers and database servers in an AWS VPC. Which of the following is a best practice in designing a multi-tier infrastructure?

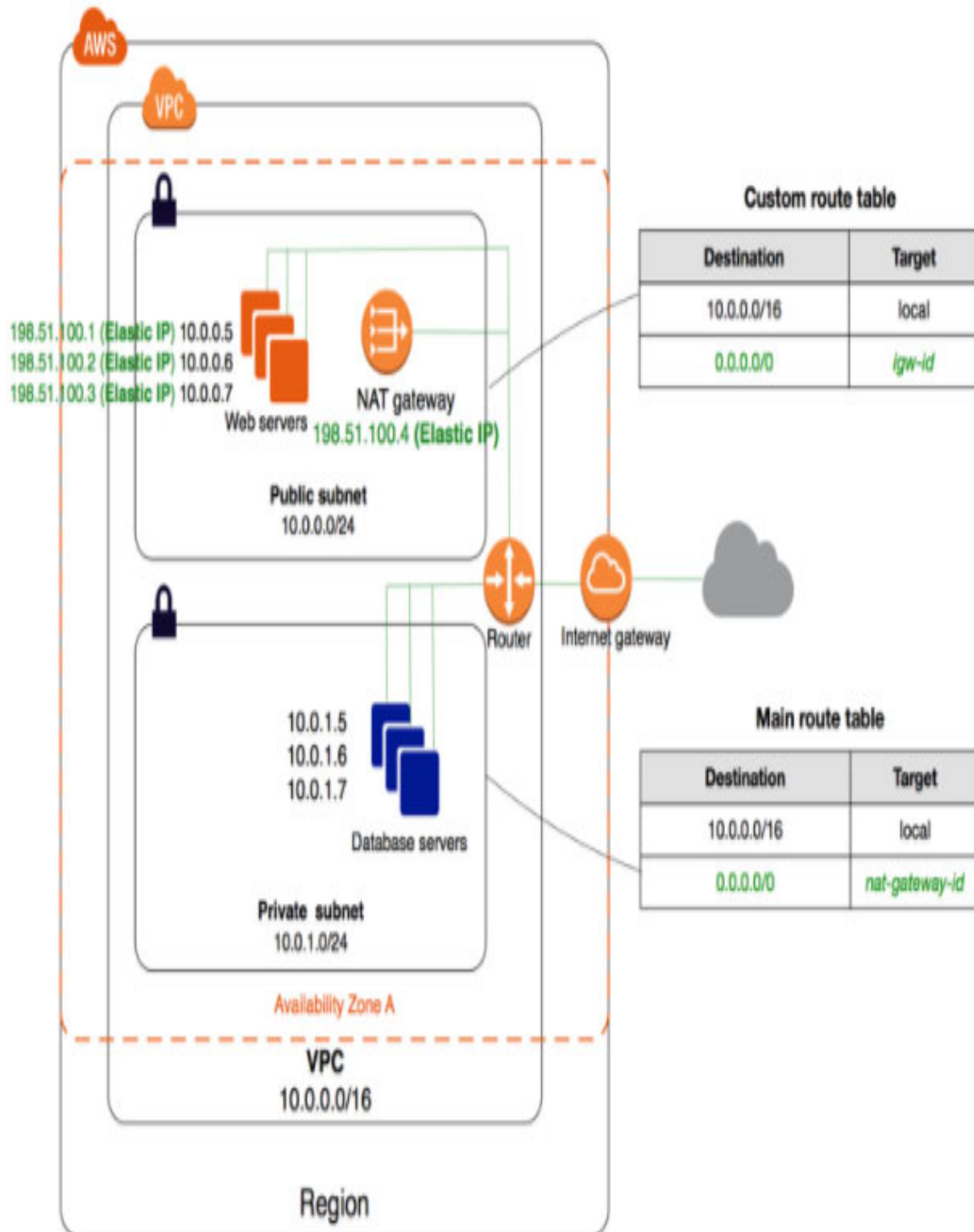
- ☐ A. Use a public subnet for the web tier and a public subnet for the database layer.
- ☒ B. Use a public subnet for the web tier and a private subnet for the database layer. ✓
- ☐ C. Use a private subnet for the web tier and a private subnet for the database layer.
- ☐ D. Use a private subnet for the web tier and a public subnet for the database layer.

## Explanation :

### Answer – B

The ideal setup is to ensure that the web server is hosted in the public subnet so that it can be accessed by users on the internet. The database server can be hosted in the private subnet.

The below diagram from AWS Documentation shows how this can be setup:





For more information on public and private subnets in AWS, please visit the following URL:  
[https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)  
([https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html))

Ask our Experts



QUESTION 61

MARKED AS REVIEW

CORRECT

SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

An IT company would like to secure their resources in their AWS Account. Which of the following options is able to secure data at rest and in transit in AWS? Choose 3 answers from the options given below.

- ☒ A. Encrypt all EBS volumes attached to EC2 Instances. ✓
- ☒ B. Use Server-Side Encryption for S3. ✓
- ☒ C. Use SSL/HTTPS when using the Elastic Load Balancer. ✓
- ☐ D. Use IOPS Volumes when working with EBS Volumes on EC2 Instances.

Explanation :

**Answer – A, B and C**

AWS documentation mentions the following:

Amazon EBS encryption offers you a simple encryption solution for your EBS volumes without the need for you to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
- Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

You can create a load balancer that uses the SSL/TLS protocol for encrypted connections (also known as *SSL offload*). This feature enables traffic encryption between your load balancer and the clients that initiate HTTPS sessions, and for connections between your load balancer and your EC2 instances.

For more information on securing data at rest, please refer to the below link:

<https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf>

(<https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf>)

Ask our Experts



QUESTION 62

CORRECT

DESIGN COST-OPTIMIZED ARCHITECTURES

Your company currently has a set of EC2 Instances running a web application which sits behind an Elastic Load Balancer. You also have an Amazon RDS instance which is accessible from the web application. You have been asked to ensure that this architecture is self-healing in nature and cost-effective. Which of the following would fulfill this requirement? Choose 2 answers from the options given below.

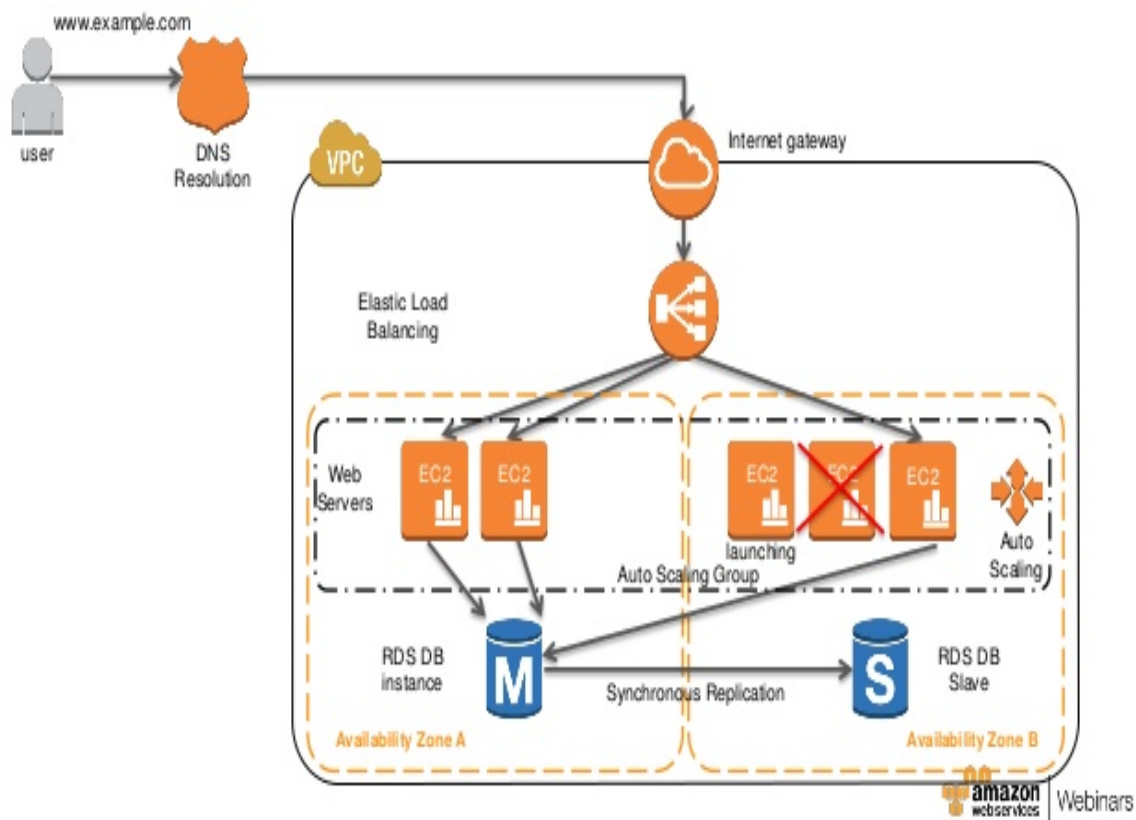
- ☒ A. Use CloudWatch metrics to check the utilization of the web layer. Use Auto Scaling Group to scale the web instances accordingly based on the CloudWatch metrics. ✓

- ☐ B. Use CloudWatch metrics to check the utilization of the databases servers. Use Auto Scaling Group to scale the database instances accordingly based on the CloudWatch metrics.
- ☐ C. Utilize the Read Replica feature for the Amazon RDS layer.
- ☒ D. Utilize the Multi-AZ feature for the Amazon RDS layer. ✓

Explanation :

Answer - A and D

The following diagram from AWS showcases a self-healing architecture where you have a set of EC2 servers as Web server being launched by an Auto Scaling Group.



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. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

For more information on Multi-AZ RDS, please refer to the below link:

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

Ask our Experts



QUESTION 63

CORRECT

SPECIFY SECURE APPLICATIONS AND ARCHITECTURES

Your company has a set of EC2 Instances that access data objects stored in an S3 bucket. Your IT Security department is concerned about the security of this architecture and wants you to implement the following:

- 1) Ensure that the EC2 Instance securely accesses the data objects stored in the S3 bucket
- 2) Prevent accidental deletion of objects

Which of the following would help fulfill the requirements of the IT Security department? Choose 2 answers from the options given below.

- ☐ A. Create an IAM user and ensure the EC2 Instances use the IAM user credentials to access the data in the bucket.
- ☒ B. Create an IAM Role and ensure the EC2 Instances use the IAM Role to access the data in the bucket. ✓

- ☐ C. Use S3 Cross-Region Replication to replicate the objects so that the integrity of data is maintained.
- ☒ D. Use an S3 bucket policy that ensures that MFA Delete is set on the objects in the bucket. ✓

**Explanation :**

**Answer - B and D**

AWS Documentation mentions the following:

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles

For more information on IAM Roles, please refer to the below link:

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

MFA Delete can be used to add another layer of security to S3 Objects to prevent accidental deletion of objects.

For more information on MFA Delete, please refer to the below link:

<https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/>  
(<https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/>)

Ask our Experts



QUESTION 64

CORRECT

DEFINE OPERATIONALLY-EXCELLENT ARCHITECTURES

You have a requirement to get a snapshot of the current configuration of resources in your AWS Account. Which of the following services can be used for this purpose?

- ☐ A. AWS CodeDeploy
- ☐ B. AWS Trusted Advisor
- ☒ C. AWS Config ✓
- ☐ D. AWS IAM

### Explanation :

#### Answer - C

AWS Documentation mentions the following:

With AWS Config, you can do the following:

- Evaluate your AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
- Retrieve configurations of one or more resources that exist in your account.
- Retrieve historical configurations of one or more resources.
- Receive a notification whenever a resource is created, modified, or deleted.
- View relationships between resources. For example, you might want to find all resources that use a particular security group.

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

<http://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

(<http://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>)

Ask our Experts



QUESTION 65

CORRECT

DEFINE PERFORMANT ARCHITECTURES

Your company is hosting an application in AWS. The application is read intensive and consists of a set of web servers and AWS RDS. It has been noticed that the response time of the application increases due to the load on the AWS RDS instance. Which of the following measures can be taken to scale the data tier? Choose 2 answers from the options given below.

- ☒ **A. Create Amazon DB Read Replicas. Configure the application layer to query the Read Replicas for query needs. ✓**
- ☐ **B. Use Auto Scaling to scale out and scale in the database tier.**
- ☐ **C. Use SQS to cache the database queries.**

✓ D. Use ElastiCache in front of your Amazon RDS DB to cache common queries. ✓

### Explanation :

#### Answer - A and D

AWS documentation mentions the following:

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.

For more information on AWS RDS Read Replica's, please visit the below URL:

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

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

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

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

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14732>)

## Certification

- ➔ Cloud Certification (<https://www.whizlabs.com/cloud-certification-training-courses/>)
- ➔ Java Certification (<https://www.whizlabs.com/oracle-java-certifications/>)

## Company

- ➔ Support (<https://help.whizlabs.com/hc/en-us>)
- ➔ Discussions (<http://ask.whizlabs.com/>)
- ➔ Blog (<https://www.whizlabs.com/blog/>)

- ➔ PM Certification  
(<https://www.whizlabs.com/project-management-certifications/>)
- ➔ Big Data Certification  
(<https://www.whizlabs.com/big-data-certifications/>)

## Mobile App

 Android Coming Soon

 iOS Coming Soon

## Follow us



(<https://www.facebook.com/whizlabs.software/>)



(<https://in.linkedin.com/company/whizlabs-software>)



(<https://twitter.com/whizlabs?lang=en>)



(<https://plus.google.com/+WhizlabsSoftware>)