

🏠 (<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>)
> New Practice Test I (<https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14546>) > **Report**

NEW PRACTICE TEST I

Attempt	1	Completed on	Monday , 28 January 2019 , 06:13 PM
Marks Obtained	0 / 60	Time Taken	00 H 00 M 07 S
Your score is	0.0%	Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	60	0	0	60

60 Questions	0 Correct	0 Incorrect	60 Unattempted	Show Answers	All	▼
-----------------	--------------	----------------	-------------------	--------------	-----	---

QUESTION 1 UNATTEMPTED

You currently have an EC2 instance hosting a web application. The number of users is expected to increase in the coming months and hence you need to add more elasticity to your setup. Which of the following methods can help add elasticity to your existing setup. Choose 2 answers from the options given below

- ☐ A. Setup your web app on more EC2 instances and set them behind an Elastic Load Balancer ✓
- ☐ B. Setup an Elastic Cache in front of the EC2 instance.
- ☐ C. Setup your web app on more EC2 instances and use Route53 to route requests accordingly. ✓
- ☐ D. Setup DynamoDB behind your EC2 Instances

Explanation :

Answer – A and C

The Elastic Load balancer is one of the most ideal solutions for adding elasticity to your application. The below snapshot is an example where you can add 3 EC2 Instances to an ELB. All requests can then be routed accordingly to these instances.

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-1bd7b87f (172.31.0.0/16)

<input type="checkbox"/>	Instance	Name	State	Security groups
<input type="checkbox"/>	i-0961c42b...	Net	stopped	WebServer
<input checked="" type="checkbox"/>	i-0d4c2602...	ServerB	running	Ubuntu
<input checked="" type="checkbox"/>	i-0d59c00d...	ServerC	running	Ubuntu
<input checked="" type="checkbox"/>	i-06f0dfa90...	ServerA	running	Ubuntu

Availability Zone Distribution

1 instance in ap-southeast-1a

2 instances in ap-southeast-1b

☒ Enable Cross-Zone Load Balancing ⓘ

☒ Enable Connection Draining ⓘ 300 seconds

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

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

The other alternative is to create a routing policy in Route53 with the Weighted routing policy.

Weighted resource record sets let you associate multiple resources with a single DNS name. Weighted routing policy enables Route 53 to route traffic to different resources in specified proportions (weights). To create a group of weighted resource record sets, two or more resource record sets can be created that have the same combination of DNS name and type, and each resource record set is assigned a unique identifier and a relative weight.

For more information on Route53, please visit the below URL:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>

(<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>)

Option B is not valid because this will just cache the reads, and will not add that desired elasticity to your application.

Option D is not valid, because there is no mention of a persistence layer in the question, that would require the use of DynamoDB.

Ask our Experts



QUESTION 2 UNATTEMPTED

You are creating a Provisioned IOPS volume in AWS. The size of the volume is 8 GiB. Which of the following are the possible values that can put for the IOPS of the volume

- ☒ A. 400 ✓
- ☐ B. 500
- ☐ C. 600
- ☐ D. 1000



Explanation :

Answer – A

The Maximum ratio of IOPS to volume size is 50:1, so if the volume size is 8 GiB, the maximum IOPS of the volume can be 400. If you go beyond this value, you will get an error as shown in the screenshot below.

```
},  
{  
  "Sid": "Allow use of the key",  
  "Effect": "Allow",  
  "Principal": {"AWS": [  
    "arn:aws:iam::111122223333:user/KMSUser",  
    "arn:aws:iam::111122223333:role/KMSRole",  
    "arn:aws:iam::444455556666:root"  
  ]},  
  "Action": [  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:ReEncrypt*",  
    "kms:GenerateDataKey*",  
    "kms:DescribeKey"  
  ],  
  "Resource": "*" ,  
}
```

For more information on Provisioned IOPS, please visit the below URL:

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

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

Ask our Experts



QUESTION 3 UNATTEMPTED

A company is hosting EC2 instances which focuses on work-loads are on non-production and non-priority batch loads. Also these processes can be interrupted at any time. What is the best pricing model which can be used for EC2 instances in this case?

- ☐ A. Reserved Instances
- ☐ B. On-Demand Instances
- ☒ C. Spot Instances ✓
- ☐ D. Regular Instances

Explanation :

Answer – C



Spot instances enable you to bid on unused EC2 instances, which can lower your Amazon EC2 costs significantly. The hourly price for a Spot instance (of each instance type in each Availability Zone) is set by Amazon EC2, and fluctuates depending on the supply of and demand for Spot instances. Your Spot instance runs whenever your bid exceeds the current market price.

Spot instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. For example, Spot instances are well-suited for data analysis, batch jobs, background processing, and optional tasks

Option A is invalid because even though Reserved instances can reduce costs, its best for workloads that would be active for a longer period of time rather than for batch load processes which could last for a shorter period of time.

Option B is not right because On-Demand Instances tend to be more expensive than Spot Instances.

Option D is invalid because there is no concept of Regular instances in AWS

For more information on Spot Instances, please visit the below URL:

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

(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html>)

Ask our Experts



QUESTION 4 UNATTEMPTED

You have 2 Ubuntu instances located in different subnets in the same VPC. Now to your understanding these instances should be able to communicate with each other, but when you try to ping from one instance to another, you get a timeout. The Route tables seem to be valid and has the entry for the Target 'local' for your VPC CIDR. Which of the following could be a valid reason for this issue.

- ☐ A. The Instances are of the wrong AMI, hence you are not able to ping the instances.
- ☐ B. The Security Group has not been modified for allow the required traffic. ✓
- ☐ C. The Instances don't have Public IP, so that the ping commands can be routed
- ☐ D. The Instances don't have Elastic IP, so that the ping commands can be routed

Explanation :

Answer – B

The security groups need to be configured to ensure that ping commands can go through. The below snapshot shows that the ICMP protocol needs to be allowed to ensure that the ping packets can be routed to the instances. You need to edit the Inbound Rules of the Web Security Group.



Configuring Amazon Route 53 to Route Traffic to an ELB Load Balancer

To configure Amazon Route 53 to route traffic to an ELB load balancer, perform the following procedure.

To route traffic to an ELB load balancer

1. If you created the Route 53 hosted zone and ELB load balancer using the same account, skip to step 2.

If you created the hosted zone and the ELB load balancer using different accounts, perform the procedure [Getting the DNS Name for an ELB Load Balancer](#) to get the DNS name for the load balancer.

2. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.

3. In the navigation pane, choose **Hosted Zones**.

4. Choose the name of the hosted zone that has the domain name that you want to use to route traffic to your load balancer.

5. Choose **Create Record Set**.

6. Specify the following values:

Name

Enter the domain name that you want to use to route traffic to your ELB load balancer. The default value is the name of the hosted zone.

For example, if the name of the hosted zone is example.com and you want to use acme.example.com to route traffic to your load balancer, enter acme.

Type

Choose A – IPv4 address.

Alias

Choose Yes.

Alias Target

If you created the hosted zone and the ELB load balancer using the same AWS account – Find the applicable category in the list (ELB Application Load Balancers, ELB Classic Load Balancers, or ELB Network Load Balancers), and then choose the name that you assigned to the load balancer when you created it.

If you created the hosted zone and the ELB load balancer using different accounts – Enter the value that you got in step 1 of this procedure.

Routing Policy

Accept the default value of Simple.

Option A is invalid because the AMI will not impact the ping command.

Public IP or Elastic IP of the instances are used to communicate with internet. However for the instances to communicate with the internet, the route table should be configured appropriately to allow traffic through Internet Gateway. We also need to make sure that appropriate inbound rules are set up in the Security Group of these instances too.

So in our scenario we are dealing with instances with in the VPC to communicate each other. So if we haven't configured the inbound ICMP traffic for these instances on the Security group of these instances then it won't allow the traffic.

So option C and D are incorrect.

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

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Ask our Experts



QUESTION 5 UNATTEMPTED

What is the best way to move an EBS volume currently attached to an EC2 instance from one availability zone to another ?

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

Explanation :



Answer – C

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

AWS: Denies Access to AWS Based on the Source IP

This example shows how you might create a policy that denies access to all AWS actions in the account when the request comes from outside the specified IP range. The policy is useful when the IP addresses for your company are within the specified ranges. This policy also provides the permissions necessary to complete this action on the console. To use this policy, replace the red text in the example policy with your own information.

The `aws:SourceIp` condition key denies access to an AWS service, such as AWS CloudFormation, that makes calls on your behalf. For more information about using the `aws:SourceIp` condition key, see [AWS Global Condition Context Keys](#).

Important

This policy does not allow any actions. Use this policy in combination with other policies that allow specific actions.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24",
          "203.0.113.0/24"
        ]
      }
    }
  }
}
```

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

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

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

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

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

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

Ask our Experts



QUESTION 6 UNATTEMPTED

When it comes to API credentials, what is the best practise recommended by AWS?

- ☒ A. Create a role which has the necessary and can be assumed by the EC2 instance. ✓
- ☐ B. Use the API credentials from an EC2 instance.
- ☐ C. Use the API credentials from a bastion host.
- ☐ D. Use the API credentials from a NAT Instance.

Explanation :

Answer – A

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

Option B,C and D are invalid because it is not secure to use API credentials from any EC2 instance. The



API credentials can be tampered with and hence is not the ideal secure way to make API calls. For more information on IAM roles for EC2, please visit the below URL:
<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>)

Ask our Experts



QUESTION 7 UNATTEMPTED

You want to retrieve the Public IP addresses assigned to a running instance via the Instance metadata. Which of the below urls is valid for retrieving this data.

- ☐ A. <http://169.254.169.254/latest/meta-data/public-ipv4> ✓
- ☐ B. <http://254.169.254.169/latest/meta-data/public-ipv4>
- ☐ C. <http://254.169.254.169/meta-data/latest/public-ipv4>
- ☐ D. <http://169.254.169.254/meta-data/latest/public-ipv4>

Explanation :

Answer - A

As per the AWS documentation, below is the right way to access the instance metadata

Characteristic	Relational Database Management System (RDBMS)	Amazon DynamoDB
Optimal Workloads	Ad hoc queries; data warehousing; OLAP (online analytical processing).	Web-scale applications, including social networks, gaming, media sharing, and IoT (Internet of Things).
Data Model	The relational model requires a well-defined schema, where data is normalized into tables, rows and columns. In addition, all of the relationships are defined among tables, columns, indexes, and other database elements.	DynamoDB is schemaless. Every table must have a primary key to uniquely identify each data item, but there are no similar constraints on other non-key attributes. DynamoDB can manage structured or semi-structured data, including JSON documents.

For more information on Instance metadata, please visit the below URL:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>)

Ask our Experts



QUESTION 8 UNATTEMPTED



You are planning to use the MySQL RDS in AWS. You have a requirement to ensure that you are available to recover from a database crash. Which of the below is not a recommended practise when you want to fulfil this requirement

- ☐ A. Ensure that automated backups are enabled for the RDS
- ☒ B. Ensure that you use the MyISAM storage engine for MySQL ✓
- ☐ C. Ensure that tables in the database do not get too large.
- ☐ D. Ensure that file sizes for the RDS is well under 16 TB.

Explanation :

Answer – B

Below is the best recommended practices for MySQL

AWS Lambda Resource Limits per Invocation

Resource	Limits
Memory allocation range	Minimum = 128 MB / Maximum = 3008 MB (with 64 MB increments). If the maximum memory use is exceeded, function invocation will be terminated.
Ephemeral disk capacity ("/tmp" space)	512 MB
Number of file descriptors	1,024
Number of processes and threads (combined total)	1,024
Maximum execution duration per request	300 seconds
Invoke request body payload size (RequestResponse/synchronous invocation)	6 MB
Invoke request body payload size (Event/asynchronous invocation)	128 K

For more information on best practices for MySQL Storage, please visit the below URL:

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html#CHAP_BestPractices.MySQLStorage
(http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_BestPractices.html#CHAP_BestPractices.MySQLStorage)

Ask our Experts



QUESTION 9 UNATTEMPTED

Which of the following is a valid bucket name

- ☒ A. demo ✓
- ☐ B. Example
- ☐ C. .example
- ☐ D. demo.

Explanation :

Answer - A

Following are the restrictions when naming buckets in S3.

- Bucket names must be at least 3 and no more than 63 characters long.



- Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period (.). Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number.
- Bucket names must not be formatted as an IP address (e.g., 192.168.5.4).
- When using virtual hosted-style buckets with SSL, the SSL wildcard certificate only matches buckets that do not contain periods. To work around this, use HTTP or write your own certificate verification logic. We recommend that you do not use periods (".") in bucket names.

Option B is invalid because it has an upper case character

Option C is invalid because the bucket name cannot start with a period (.).

Option D is invalid because the bucket name cannot end with a period (.).

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

<http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html>

(<http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html>)

Ask our Experts



QUESTION 10 UNATTEMPTED

Which of the following is not a feature provided by Route53?

- ☐ A. Registration of Domain Names
- ☐ B. Routing of internet traffic to domain resources
- ☒ C. Offloading content to cache locations ✓
- ☐ D. Health check of resources

Explanation :

Answer – C

The below features are available for Route53 hence option A,B and D are valid.

- Register domain names – Your website needs a name, such as example.com. Amazon Route 53 lets you register a name for your website or web application, known as a domain name.
- Route internet traffic to the resources for your domain – When a user opens a web browser and enters your domain name in the address bar, Amazon Route 53 helps the Domain Name System (DNS) connect the browser with your website or web application.
- Check the health of your resources – Amazon Route 53 sends automated requests over the internet to a resource, such as a web server, to verify that it's reachable, available, and functional. You also can choose to receive notifications when a resource becomes unavailable and choose to route internet traffic away from unhealthy resources.

Option C is basically a feature provided by the AWS Content Delivery service.

For more information on Route53, please visit the below URL:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>

(<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html>)

Ask our Experts



QUESTION 11

UNATTEMPTED

When working with API gateways in AWS , what is the type of endpoints that are exposed

- ☐ A. HTTP
- ☒ B. HTTPS ✓
- ☐ C. JSON
- ☐ D. XML

Explanation :

Answer - B

All of the endpoints created with the API gateway are of HTTPS.

Option A is incorrect because Amazon API Gateway does not support unencrypted (HTTP) endpoints

Option C and D are invalid because API gateway expose HTTPS endpoints only

For more information on API Gateways, please visit the below URL:

<https://aws.amazon.com/api-gateway/faqs/> (<https://aws.amazon.com/api-gateway/faqs/>)

Ask our Experts



QUESTION 12

UNATTEMPTED

Which of the following verbs are supported with the API Gateway

- ☐ A. GET
- ☐ B. POST
- ☐ C. PUT
- ☒ D. All of the above ✓

Explanation :

Answer - D

Each resource within a REST API can support one or more of the standard HTTP methods. You define which verbs should be supported for each resource (GET, POST, PUT, PATCH, DELETE, HEAD, OPTIONS) and their implementation.

For more information on API Gateways, please visit the below URL:

<https://aws.amazon.com/api-gateway/faqs/> (<https://aws.amazon.com/api-gateway/faqs/>)

Ask our Experts



QUESTION 13

UNATTEMPTED

Which of the following container technologies are currently supported by the AWS



ECS service?

- ☐ A. Kubernetes
- ☒ B. Docker ✓
- ☐ C. Mesosphere
- ☐ D. Canonical LXD

Explanation :

Answer - Option B

Docker is a technology that allows you to build, run, test, and deploy distributed applications that are based on Linux containers.

Kubernetes is a container orchestration system for Docker containers. So its incorrect.

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

- <https://aws.amazon.com/containers/new/> (<https://aws.amazon.com/containers/new/>)
- <https://aws.amazon.com/ecs/faqs/> (<https://aws.amazon.com/ecs/faqs/>)
- <https://aws.amazon.com/blogs/aws/amazon-elastic-container-service-for-kubernetes/> (<https://aws.amazon.com/blogs/aws/amazon-elastic-container-service-for-kubernetes/>)

Ask our Experts



QUESTION 14 UNATTEMPTED

Which of the following when used alongside with the AWS Secure Token service can be used to provide a single sign-on experience for existing users who are part of an organization using on-premise applications

- ☐ A. OpenID Connect
- ☐ B. JSON
- ☒ C. SAML 2.0 ✓
- ☐ D. OAuth

Explanation :

Answer - C



You can authenticate users in your organization's network, and then provide those users access to AWS without creating new AWS identities for them and requiring them to sign in with a separate user name and password. This is known as the single sign-on (SSO) approach to temporary access. AWS STS supports open standards like Security Assertion Markup Language (SAML) 2.0, with which you can use Microsoft AD FS to leverage your Microsoft Active Directory.

Option A and D are incorrect because these are used when you want users to sign in using a well-known third party identity provider such as Login with Amazon, Facebook, Google.

Option B is incorrect because this is more of a data exchange protocol.

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

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

Ask our Experts



QUESTION 15 UNATTEMPTED

While performing status checks on your volume in AWS, you can see that the volume check has a status of "insufficient-data". What can you derive from this status check

- ☐ A. All checks have passed
- ☐ B. A particular check has failed only
- ☐ C. All checks have failed
- ☒ D. The check on the volume is still in progress. ✓

Explanation :

Answer - D

Volume status checks enable you to better understand, track, and manage potential inconsistencies in the data on an Amazon EBS volume. They are designed to provide you with the information that you need to determine whether your Amazon EBS volumes are impaired, and to help you control how a potentially inconsistent volume is handled.

If the status is insufficient-data, the checks may still be in progress on the volume.

Option A is incorrect because if all checks have passed, then the status of the volume is OK.

Option B and C are incorrect because if a check fails, then the status of the volume is impaired

For more information on Volume status checks, please visit the below URL:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html>

(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html>)

Ask our Experts



QUESTION 16 UNATTEMPTED

Which of the following can constitute the term of a 'Golden Image'

- ☐ A. This is the basic AMI which is available in AWS.
- ☐ B. This refers to an instance which has been bootstrapped.



- ☐ C. This refers to an AMI that has been constructed from a customized Image. ✓
- ☐ D. This refers to a special type of Linux AMI.

Explanation :

Answer - C

You can customize an Amazon EC2 instance and then save its configuration by creating an Amazon Machine Image (AMI). You can launch as many instances from the AMI as you need, and they will all include those customizations that you've made. Each time you want to change your configuration you will need to create a new golden image, so you will need to have a versioning convention to manage your golden images over time

Because of the above explanation , all of the remaining options are automatically invalid.

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

- <https://aws.amazon.com/blogs/awsmarketplace/announcing-the-golden-ami-pipeline/>
(<https://aws.amazon.com/blogs/awsmarketplace/announcing-the-golden-ami-pipeline/>)
- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>)

Ask our Experts



QUESTION 17 UNATTEMPTED

When designing a health check for your web application which is hosted behind an elastic load balancer, which of the following health checks is ideal to implement

- ☐ A. A TCP health check
- ☐ B. A UDP health check
- ☐ C. A HTTP health check ✓
- ☐ D. A combination of TCP and UDP health checks

Explanation :

Answer - C

Option B and D is invalid because UDP health checks are not possible

Option A is partially valid. A simple TCP health check would not detect the scenario where the instance itself is healthy, but the web server process has crashed. Instead, you should assess whether the web server can return a HTTP 200 response for some simple request.

For more information on ELB health checks, please visit the below URL:

<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>
(<http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-healthchecks.html>)

Ask our Experts



QUESTION 18 UNATTEMPTED



Which of the following is an example of synchronous replication which occurs in the AWS service?

- ☐ A. AWS RDS Read Replica's for MySQL, MariaDB and PostgreSQL
- ☒ B. AWS Multi-AZ RDS ✓
- ☐ C. Redis engine for Amazon ElastiCache replication
- ☐ D. AWS RDS Read Replica's for Oracle

Explanation :

Answer - B

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).

For more information on Multi-AZ, please visit the below URL:

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

Option A is invalid because Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. For MySQL, MariaDB and PostgreSQL, Amazon RDS uses those engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance.

Option C is invalid, because the Redis engine for Amazon ElastiCache supports replication with automatic failover, but the Redis engine's replication is asynchronous

Option D is invalid because this is not supported by AWS.

Ask our Experts



QUESTION 19 UNATTEMPTED

You want to get the reason for your EC2 Instance termination from the CLI. Which of the below commands is ideal in getting the reason.

- ☒ A. `aws ec2 describe-instances` ✓
- ☐ B. `aws ec2 describe-images`
- ☐ C. `aws ec2 get-console-screenshot`
- ☐ D. `aws ec2 describe-volume-status`

Explanation :

Answer - A

When you execute the AWS `ec2 describe-instances` CLI command with the `instance_id` as shown below

`aws ec2 describe-instances --instance-id instance_id`

In the JSON response that's displayed, locate the `StateReason` element.

An example is shown below. This will help in understanding why the instance was shutdown.

"StateReason": {



```
"Message": "Client.UserInitiatedShutdown: User initiated shutdown",
"Code": "Client.UserInitiatedShutdown"
},
```

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

<http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>

(<http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html>)

Option B is invalid because this command describes one or more of the images (AMIs, AKIs, and ARIs) available to you

Option C is invalid because retrieve a JPG-format screenshot of a running instance. This might not help to the complete extent of understanding why the instance was terminated.

Option D is invalid because this command describes the status of the specified volumes.

Ask our Experts



QUESTION 20 UNATTEMPTED

When using the following AWS services, which should be implemented in multiple Availability Zones for high availability solutions?

Choose 2 answers from the options below.

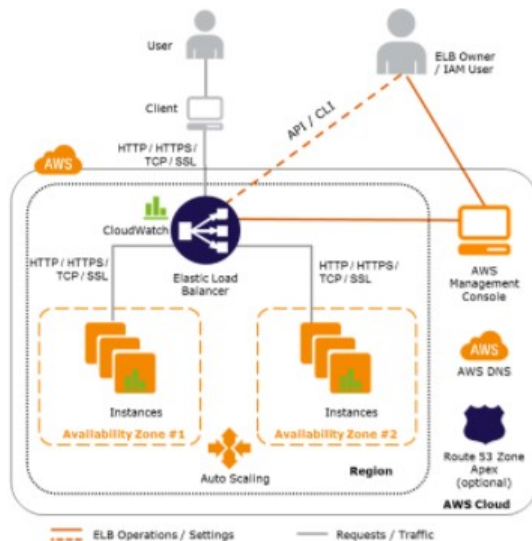
- ☐ A. Amazon DynamoDB
- ☐ B. Amazon Elastic Compute Cloud (EC2) ✓
- ☐ C. Amazon Elastic Load Balancing ✓
- ☐ D. Amazon Simple Storage Service (S3)

Explanation :

Answer – B and C

The below snapshot from the AWS documentation shows how the ELB and EC2 instances get setup for high availability. You have the ELB placed in front of the instances. The instances are placed in different AZ's.





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

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

Option A is wrong because the service runs across Amazon's proven, high-availability data centers.

The service replicates data across three facilities in an AWS Region to provide fault tolerance in the event of a server failure or Availability Zone outage.

Option D is wrong because Amazon S3 Standard and Standard - IA redundantly stores your objects on multiple devices across multiple facilities in an Amazon S3 Region. The service is designed to sustain concurrent device failures by quickly detecting and repairing any lost redundancy

Note:

AWS says as mentioned below:

"When you enable an Availability Zone for your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. If you register targets in an Availability Zone but do not enable the Availability Zone, these registered targets do not receive traffic. Note that your load balancer is most effective if you ensure that each enabled Availability Zone has at least one registered target.

We recommend that you enable multiple Availability Zones. (Note that with an Application Load Balancer, we require you to enable multiple Availability Zones.) With this configuration, if one Availability Zone becomes unavailable or has no healthy targets, the load balancer can continue to route traffic to the healthy targets in another Availability Zone."

So, we need to enable multiple Availability Zones for load balancer as well.

We do have control over which AZ the load balancer is deployed to. For example in Singapore (ap-southeast-1) region we do have 3 availability zone, we could create one load balancer and load balance between any 2 AZ out of 3.

AWS says as mentioned below:

"Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer."

Ask our Experts



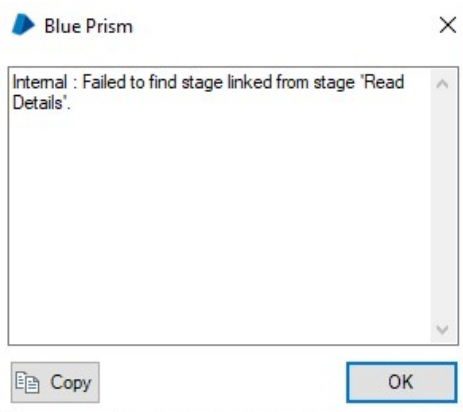
An application is currently configured on an EC2 instance to process messages in SQS. The queue has been created with the default settings. The application is configured to just read the messages once a week. It has been noticed that not all the messages are being picked by the application. What could be the issue?

- ☐ A. The application is configured to long polling, so some messages are not being picked up
- ☐ B. The application is configured to short polling, so some messages are not being picked up
- ☒ C. Some of the messages have surpassed the retention period defined for the queue ✓
- ☐ D. Some of the messages don't have the right permissions to be picked up by the application

Explanation :

Answer - C

When you create an SQS with the default options, the message retention period is 4 days. So if the application is processing the messages just once a week there are chances that messages sent at the start of the week will get deleted before it can be picked up by the application.



Option A and B are invalid, because even if you use short or long polling, the application should be able to read the messages eventually.

Option D is invalid because you can provide permissions at the queue level.

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

<https://aws.amazon.com/sqs/faqs/> (<https://aws.amazon.com/sqs/faqs/>)

Ask our Experts



Your application is on an EC2 instance in AWS. Users use the application to upload a file to S3. The message first goes to an SQS queue, before it is picked up by a worker process, which fetches the object and uploads it to S3. An email is then sent on



successful completion of the upload. You notice though that you are getting numerous emails for each request, when ideally you should be getting only one final email notification for each successful upload. Which of the below could be the possible reasons for this.

- ☐ A. The application is configured for long polling so the messages are being picked up multiple times.
- ☐ B. The application is not deleting the messages from SQS. ✓
- ☐ C. The application is configured to short polling, so some messages are not being picked up
- ☐ D. The application is not reading the message properly from the SQS queue.

Explanation :

Answer – B

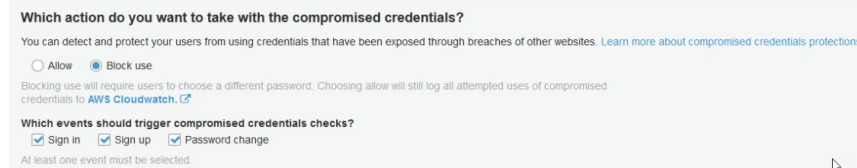
When you look at the Message lifecycle from AWS for SQS queues , one of the most important aspect is to delete the messages after they have been read from the queue.

Checking for Compromised Credentials

Amazon Cognito can detect if a user's credentials (user name and password) have been compromised elsewhere. This can happen when users reuse credentials at more than one site, or when they use passwords that are easy to guess.

From the **Advanced security** page in the Amazon Cognito console, you can choose whether to allow, or block the user if compromised credentials are detected. Blocking requires users to choose another password. Choosing **Allow** publishes all attempted uses of compromised credentials to Amazon CloudWatch. For more information, see [Viewing Advanced Security Metrics](#).

You can also choose whether Amazon Cognito checks for compromised credentials during sign-in, sign-up, and password changes.



Which action do you want to take with the compromised credentials?

You can detect and protect your users from using credentials that have been exposed through breaches of other websites. [Learn more about compromised credentials protections.](#)

☐ Allow ☒ Block use

Blocking use will require users to choose a different password. Choosing allow will still log all attempted uses of compromised credentials to [AWS Cloudwatch](#).

Which events should trigger compromised credentials checks?

☒ Sign in ☒ Sign up ☒ Password change

At least one event must be selected.

Option A and C are invalid because even if you use short or long polling , the application should be able to read the messages eventually. The main part is that the deletion of messages is not happening after they have been read.

Option D is invalid because if the messages are not being read properly , then the application should not send successful notifications.

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

<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>

(<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-message-lifecycle.html>)

Ask our Experts



QUESTION 23 UNATTEMPTED

You have created your own VPC and subnet in AWS. You have launched an instance in that subnet. You have noticed that the instance is not receiving a DNS name. Which of the below options could be a valid reason for this issue.



- ☐ A. The CIDR block for the VPC is invalid
- ☐ B. The CIDR block for the subnet is invalid
- ☒ C. The VPC configuration needs to be changed. ✓
- ☐ D. The subnet configuration needs to be changed.

Explanation :

Answer – C

If the DNS hostnames option of the VPC is not set to 'Yes' then the instances launched in the subnet will not get DNS Names.

Type	Protocol	Port Range	Source	Description
HTTP (80)	TCP (6)	80	10.10.1.148/32	
HTTP (80)	TCP (6)	80	10.10.1.0/28	
ALL TCP	TCP (6)	ALL	10.10.1.148/32	
SSH (22)	TCP (6)	22	10.10.1.0/28	
Custom UDP Rule	UDP (17)	3000	10.10.1.148/32	

You can change the option by choosing your VPC and clicking on 'Edit DNS Hostnames'



Option A and B are invalid because if the CIDR blocks were invalid then the VPC or subnet would not be created.

Option D is invalid because the subnet configuration does not have the effect on the DNS hostnames.

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

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

Ask our Experts



QUESTION 24 UNATTEMPTED

You have created your own VPC and subnet in AWS. You have launched an instance in that subnet. You have attached an internet gateway to the VPC and seen that the instance has a public IP. The Route table is shown below



Summary	Routes	Subnet Associations	Route Propagation	Tags
---------	---------------	---------------------	-------------------	------

Edit

View: All rules ▾

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

The instance still cannot be reached from the Internet. Which of the below changes need to be made to the route table to ensure that the issue can be resolved.

- ☐ A. Add the following entry to the route table – 0.0.0.0/0->Internet Gateway ✓
- ☐ B. Modify the above route table – 10.0.0.0/16 ->Internet Gateway
- ☐ C. Add the following entry to the route table – 10.0.0.0/16 ->Internet Gateway
- ☐ D. Add the following entry to the route table - 0.0.0.0/16->Internet Gateway

Explanation :

Answer – A

The Route table need to be modified as shown below to ensure that the routes from the internet can reach the instance

Summary	Routes	Subnet Associations	Route Propagation	Tags
---------	---------------	---------------------	-------------------	------

Edit ✓ Save Successful

View: All rules ▾

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-a97272cc	Active	No

Hence by default all other options become invalid

For more information on Route Tables, please visit the below URL:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)

Note:

In order to be routable to internet, we must add 0.0.0.0/0 (internet) as the destination and target (internet gateway). We can interpret the configuration in a simple statement:

In order to reach internet (0.0.0.0/0), we must route all the traffic through the internet gateway (target).

You may refer to the link below for more info:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html)

Ask our Experts



You wanted to have a VPC created in AWS which will host an application. The application will just consist of web and database servers. The application just requires to be accessed from the internet by internet users. Which of the following VPC configuration wizards options would you use

- ☐ A. VPC with a Single Public Subnet Only
- ☒ B. VPC with Public and Private Subnets ✓
- ☐ C. VPC with Public and Private Subnets and Hardware VPN Access
- ☐ D. VPC with a Private Subnet Only and Hardware VPN Access

Explanation :

Answer – B

The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application, while maintaining back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.

Option A is invalid , because ideally you need a private subnet to host the database server.

Option C and D are invalid because there is no case of accessing the application from on-premise locations using VPN connections.

For more information on this scenario, please visit the below URL:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts



Which of the following statements are true with regards to EBS Volumes. Choose 3 correct answers from the options given below

- ☒ A. EBS Volumes are automatically replicated within that zone to prevent data loss due to failure of any single hardware component ✓
- ☒ B. EBS Volumes can be attached to any EC2 Instance in any AZ.
- ☒ C. After you attach a volume, it appears as a native block device similar to a hard drive or other physical device. ✓
- ☒ D. An EBS volume can be attached to only one instance at a time ✓

Explanation :

Answer - A, C and D



When you create an EBS volume in an Availability Zone, it is automatically replicated within that zone to prevent data loss due to failure of any single hardware component. After you create a volume, you can attach it to any EC2 instance in the same Availability Zone. After you attach a volume, it appears as a native block device similar to a hard drive or other physical device. At that point, the instance can interact with the volume just as it would with a local drive; the instance can format the EBS volume with a file system, such as ext3, and then install applications.

An EBS volume can be attached to only one instance at a time within the same Availability Zone.

However, multiple volumes can be attached to a single instance.

Option B is invalid because you can attach EBS Volumes to any EC2 instance in the same Availability Zone only

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

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

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

Ask our Experts



QUESTION 27 UNATTEMPTED

You are a solutions architect working for a large oil and gas company. Your company runs their production environment on AWS and has a custom VPC. The VPC contains 3 subnets, 1 of which is public and the other 2 are private. Inside the public subnet is a fleet of EC2 instances which are the result of an autoscaling group. All EC2 instances are in the same security group. Your company has created a new custom application which connects to mobile devices using a custom port. This application has been rolled out to production and you need to open this port globally to the internet. What steps should you take to do this, and how quickly will the change occur?

- ☐ A. Open the port on the existing network Access Control List. Your EC2 instances will be able to communicate on this port after a reboot.
- ☐ B. Open the port on the existing network Access Control List. Your EC2 instances will be able to communicate over this port immediately.
- ☐ C. Open the port on the existing security group. Your EC2 instances will be able to communicate over this port immediately. ✓
- ☐ D. Open the port on the existing security group. Your EC2 instances will be able to communicate over this port as soon as the relevant Time To Live (TTL) expires.

Explanation :

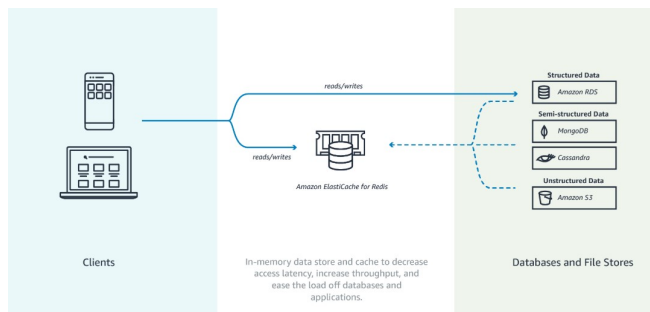
Answer – C

One can use the Security Group , change the Inbound Rules so that the traffic will be allowed on the custom port.

When you make a change to the Security Groups or Network ACL's , they are applied immediately

This is clearly given in the AWS documentation





There is insufficient information for us to conclude that we should open the port on the NACL in this question. Likewise, for example if one of the option mentioned "Enable the windows firewall to allow the connection" is also out of our consideration due to insufficient of data to make judgement and best choice.

In the exam, you will encounter question like this, you should always focus on the details given in the question, choose the best possible solution from the answer options without making own assumption.

So in this question, the best choice is C.

For more information on Security Groups, please refer to the below link

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Note:

A security group acts as a virtual firewall that controls the traffic for one or more instances.

Security groups are stateful – if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

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.

ACL's are stateless, responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

In our question we haven't mentioned anything specific about ACLs. So let us assume that we are using the default ACL for our custom VPC. By default, it allows all inbound and outbound IPv4 traffic. This will ensure that at subnet level the traffic is not blocked to any of the instances.

The next step is to make sure that the Security Group should allow traffic to flow through the desired port. Any changes to Security Group rules are immediately applied to the instances. Hence Option C is the suitable one in this scenario.

More information on Security Group Basics and ACLs are available at:

- 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_ACLs.html#nacl-examples
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#nacl-examples)

Ask our Experts



You are designing various CloudFormation templates, each template to be used for a different purpose. What determines the cost of using the CloudFormation templates?

- ☒ A. CloudFormation does not have a cost itself. ✓
- ☐ B. You are charged based on the size of the template.
- ☐ C. You are charged based on the time it takes to launch the template.
- ☐ D. It has a basic charge of \$1.10

Explanation :

Answer – A

If you look at the AWS Documentation, this is clearly given.

ProvisionedThroughputExceededException

Message: You exceeded your maximum allowed provisioned throughput for a table or for one or more global secondary indexes. To view performance metrics for provisioned throughput vs. consumed throughput, open the Amazon CloudWatch console.

Example: Your request rate is too high. The AWS SDKs for DynamoDB automatically retry requests that receive this exception. Your request is eventually successful, unless your retry queue is too large to finish. Reduce the frequency of requests, using [Error Retries and Exponential Backoff](#).

You only get charged for the underlying resources created using Cloud Formation templates.

So, because of the explanation, all other options automatically become invalid.

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

<https://aws.amazon.com/cloudformation/faqs/> (<https://aws.amazon.com/cloudformation/faqs/>)

Ask our Experts



QUESTION 29 UNATTEMPTED

You are creating a number of EBS Volumes for your EC2 instances. You are concerned on the backups of the EBS Volumes. Which of the below is a way to backup the EBS Volumes

- ☐ A. Configure Amazon Storage Gateway with EBS volumes as the data source and store the backups on premise through the storage gateway
- ☐ B. Write a cronjob that uses the AWS CLI to take a snapshot of production EBS volumes. ✓
- ☐ C. Use a lifecycle policy to back up EBS volumes stored on Amazon S3 for durability ✓
- ☐ D. Write a cronjob on the server that compresses the data and then copy it to Glacier

Explanation :

Answer – B and C



A point-in-time snapshot of an EBS volume, can be used as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental—only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the entire volume.

You can create a snapshot via the CLI command – create-snapshot

Option A is incorrect because you normally use the Storage gateway to backup your on-premise data.

Option C is correct because Amazon Data Lifecycle Manager (DLM) for EBS Snapshots provides a simple, automated way to back up data stored on Amazon EBS volumes. You can define backup and retention schedules for EBS snapshots by creating lifecycle policies based on tags. With this feature, you no longer have to rely on custom scripts to create and manage your backups.

<https://aws.amazon.com/about-aws/whats-new/2018/07/introducing-amazon-data-lifecycle-manager-for-ebs-snapshots/> (<https://aws.amazon.com/about-aws/whats-new/2018/07/introducing-amazon-data-lifecycle-manager-for-ebs-snapshots/>)

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

Option D is incorrect because compression is another maintenance task and storing it in Glacier is not an ideal option

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

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>

(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html>)

Ask our Experts



QUESTION 30 UNATTEMPTED

You are planning on hosting a static website on an EC2 Instance. Which of the below aspects can be used to create a highly available environment. Choose 3 answers from the options given below

- ☐ A. An auto scaling group to recover from EC2 instance failures ✓
- ☐ B. Elastic Load Balancer ✓
- ☐ C. An SQS queue
- ☐ D. Multiple Availability Zones ✓

Explanation :

Answer - A,B and D

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



Lambda function

The following shows the notation you use to describe a Lambda function:

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Resources:

  FunctionName:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: runtime
      CodeUri: s3://bucketName/codepackage.zip
```

Here you have the

- 1) ELB which is placed in front of the users which helps in directing the traffic to the EC2 Instances.
 - 2) The EC2 Instances which are placed as part of an AutoScaling Group
 - 3) And then you have multiple subnets which are mapped to multiple availability zones
- For a static web site, the SQS is not required to build such an environment. If you have a system such as an order processing systems, which has that sort of queuing of requests, then that could be a candidate for using SQS Queues.

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

https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf
(https://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_ftha_04.pdf)

Ask our Experts



QUESTION 31 UNATTEMPTED

You have a set of IIS Servers running on EC2 instances for a high traffic web site. You want to collect and process the log files generated from the IIS Servers. Which of the below services is ideal to run in this scenario

- ☐ A. Amazon S3 for storing the log files and Amazon EMR for processing the log files ✓
- ☐ B. Amazon S3 for storing the log files and EC2 Instances for processing the log files
- ☐ C. Amazon EC2 for storing and processing the log files
- ☐ D. Amazon DynamoDB to store the logs and EC2 for running custom log analysis scripts

Explanation :

Answer – A

Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop (<https://aws.amazon.com/elasticmapreduce/details/hadoop>) and Apache Spark (<https://aws.amazon.com/elasticmapreduce/details/spark>), on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects, such as Apache Hive



and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move large amounts of data into and out of other AWS data stores and databases, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB.

Option B and C, even though partially correct would be an overhead for EC2 Instances to process the log files when you already have a ready made service which can help in this regard

Option D is invalid because DynamoDB is not an ideal option to store log files.

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

<http://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>

(<http://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html>)

Ask our Experts



QUESTION 32 UNATTEMPTED

You are trying to configure Cross Region Replication for your S3 bucket. But you are not able to select the option of Cross Region Replication and is disabled.

Which of the below could be the possible reasons for this ?

- ☐ A. The feature is not available in that region
- ☐ B. You need to enable versioning on the bucket ✓
- ☐ C. The source region is currently down
- ☐ D. The destination region is currently down

Explanation :

Answer – B

Requirements for cross-region replication:

- The source and destination buckets must be versioning-enabled.
- The source and destination buckets must be in different AWS regions.
- You can replicate objects from a source bucket to only one destination bucket.
- Amazon S3 must have permission to replicate objects from that source bucket to the destination bucket on your behalf.
- If the source bucket owner also owns the object, the bucket owner has full permissions to replicate the object. If not, the source bucket owner must have permission for the Amazon S3 actions `s3:GetObjectVersion` and `s3:GetObjectVersionACL` to read the object and object ACL.
- If you are setting up cross-region replication in a cross-account scenario (where the source and destination buckets are owned by different AWS accounts), the source bucket owner must have permission to replicate objects in the destination bucket.

The destination bucket owner needs to grant these permissions via a bucket policy.

Option A is invalid, because it is available in all regions

Option C is invalid because if so, then you would not be able to access S3 in that region

Option D is invalid because you have not reached the configuration stage to select the destination bucket

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

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



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

Ask our Experts



QUESTION 33 UNATTEMPTED

By using AWS Lambda with SQS, what are the things will lamda take care?
Select 2 valid options.

- ☐ A. Automatically retrieving messages and directing them to the target Lambda function. ✓
- ☐ B. Invoke new messages based on requirement.
- ☐ C. Deleting them once your Lambda function successfully completes. ✓
- ☐ D. Keep it safe your messages in SQS without deleting them.

Explanation :

Answer – A and C

Attaching an Amazon SQS queue as an AWS Lambda event source is an easy way to process the queue's content using a Lambda function. Lambda takes care of:

- Automatically retrieving messages and directing them to the target Lambda function.
- Deleting them once your Lambda function successfully completes.

Option B is wrong because Lambda invoke the functions not messages.

Option D is wrong because Lambda will delete messages once your Lambda function completes.

To get more information, please refer:

<https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html>

(<https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html>)

Ask our Experts



QUESTION 34 UNATTEMPTED

You have a requirement to create a subnet in an AWS VPC which will host around 20 hosts. This subnet will be used to host web servers. Which of the below could be the possible CIDR block allocated for the subnet

- ☐ A. 10.0.1.0/27 ✓
- ☐ B. 10.0.1.0/28
- ☐ C. 10.0.1.0/29
- ☐ D. 10.0.1.0/30



Explanation :

Answer - A

The available IP addresses for this CIDR block is 32 addresses. However the first four IP addresses and the last IP address in each subnet CIDR blocks are reserved and cannot be assigned to an instance. This is the reason why in the explanation part it has been written as 27 IP addresses are available for allocation.

10.0.1.0 - Network address

10.0.1.1 - Reserved by AWS

10.0.1.2 - Reserved by AWS

10.0.1.3 - Reserved by AWS

10.0.1.31 - Network broadcast address

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

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing

(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing)

With this configuration you can have 27 allowable hosts which fits the requirement.

Option B is invalid because you can have only a maximum of 16 hosts with this configuration

Option C and D are invalid because you can assign a single CIDR block to a VPC. The allowed block size is between a /16 netmask and /28 netmask.

Ask our Experts

**QUESTION 35 UNATTEMPTED**

You run a website which hosts videos and you have two types of members, premium fee paying members and free members. All videos uploaded by both your premium members and free members are processed by a fleet of EC2 instances which will poll SQS as videos are uploaded. However you need to ensure that your premium fee paying members videos have a higher priority than your free members. How do you design SQS?

- ☐ A. SQS allows you to set priorities on individual items within the queue, so simply set the fee paying members at a higher priority than your free members.
- ☐ B. Create two SQS queues, one for premium members and one for free members. Program your EC2 fleet to poll the premium queue first and if empty, to then poll your free members SQS queue. ✓
- ☐ C. SQS would not be suitable for this scenario. It would be much better to use SNS to encode the videos.
- ☐ D. Use SNS to notify when a premium member has uploaded a video and then process that video accordingly.

Explanation :

Answer – B

In this case, you can have multiple SQS queues. The SQS queues for the premium members can be polled first by the EC2 Instances and then those messages can be processed.



For information on SQS best practices, please refer to the below link
<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-best-practices.html>
(<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-best-practices.html>)

Ask our Experts



QUESTION 36 UNATTEMPTED

Which of the following are true about AWS Server-Side Encryption (SSE)?

Select 2 options.

- ☐ A. SSE encrypts messages as soon as Amazon SQS receives them. ✓
- ☐ B. Standard queue does not support SSE but SQS FIFO queue does support SSE.
- ☐ C. You cannot configure SSE on an existing SQS queue.
- ☐ D. SSE does not encrypt Queue metadata and Message metadata on SQS. ✓
- ☐ E. Amazon Simple Queue Service

Explanation :

Answer – A and D

SSE encrypts messages as soon as Amazon SQS receives them. The messages are stored in encrypted form and Amazon SQS decrypts messages only when they are sent to an authorized consumer.

<https://aws.amazon.com/sqs/faqs/> (<https://aws.amazon.com/sqs/faqs/>)

Option C is incorrect.

Q: How do I enable SSE for a new or existing Amazon SQS queue?

To enable SSE for a new or existing queue using the Amazon SQS API, specify the customer master key (CMK) ID: the alias, alias ARN, key ID, or key ARN of the an AWS-managed CMK or a custom CMK by setting the KmsMasterKeyId attribute of the CreateQueue or SetQueueAttributes action.

For detailed instructions, see [Creating an Amazon SQS Queue with Server-Side Encryption](#) and [Configuring Server-Side Encryption \(SSE\) for an Existing Amazon SQS Queue](#) in the *Amazon SQS Developer Guide*.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-sse-existing-queue.html>

Option D is incorrect

Q: What does SSE for Amazon SQS encrypt and how is it encrypted?

SSE encrypts the body of a message in an Amazon SQS queue.

SSE doesn't encrypt the following components:

- Queue metadata (queue name and attributes)
- Message metadata (message ID, timestamp, and attributes)
- Per-queue metrics



Note: This question is outdated. So only consider this for Old version of exam.

Ask our Experts



QUESTION 37 UNATTEMPTED

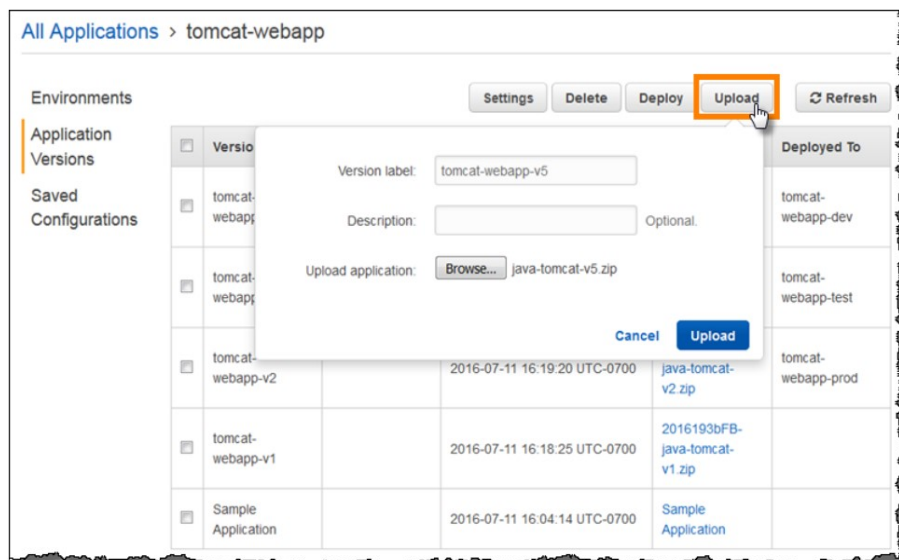
In a Custom VPC, you have launched two web servers and attached to an internet facing ELB. Both your web servers and ELB are located in the subnet. Yet, you are still not able to access your web application via the ELB's DNS through the internet. What could be done to resolve this issue?

- ☐ A. Attach an Internet gateway to the VPC and route it to the subnet ✓
- ☐ B. Add an elastic IP address to the instance
- ☐ C. Use Amazon Elastic Load Balancer to serve requests to your instances located in the internal subnet
- ☐ D. Recreate the instances again

Explanation :

Answer – A

You need to ensure that the VPC has an internet gateway attached and the route table properly configured for the subnet.



Option B is invalid because even the ELB is not accessible from the internet.

Option C is invalid because the instances and ELB is not reachable via internet if no internet gateway is attached to the VPC.

Option D is invalid because this will not have an impact on the issue.



For more information on troubleshooting ELB, please visit the below URL:
<https://aws.amazon.com/premiumsupport/knowledge-center/elb-connectivity-troubleshooting/>
(<https://aws.amazon.com/premiumsupport/knowledge-center/elb-connectivity-troubleshooting/>)

Ask our Experts



QUESTION 38 UNATTEMPTED

You want to ensure that you keep a check on the Active Volumes , Active snapshots and Elastic IP addresses you use so that you don't go beyond the service limit. Which of the below services can help in this regard?

- ☐ A. AWS Cloudwatch
- ☐ B. AWS EC2
- ☒ C. AWS Trusted Advisor ✓
- ☐ D. AWS SNS

Explanation :

Answer - C

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.

Below is a snapshot of the service limits it can monitor

Shards

A *shard* is a uniquely identified sequence of data records in a stream. A stream is composed of one or more shards, each of which provides a fixed unit of capacity. Each shard can support up to 5 transactions per second for reads, up to a maximum total data read rate of 2 MB per second and up to 1,000 records per second for writes, up to a maximum total data write rate of 1 MB per second (including partition keys). The data capacity of your stream is a function of the number of shards that you specify for the stream. The total capacity of the stream is the sum of the capacities of its shards.

If your data rate increases, you can increase or decrease the number of shards allocated to your stream.

Option A is invalid because even though you can monitor resources , it cannot be checked against the service limit.

Option B is invalid because this is the Elastic Compute cloud service

Option D is invalid because it can be send notification but not check on service limits

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

<https://aws.amazon.com/premiumsupport/ta-faqs/> (<https://aws.amazon.com/premiumsupport/ta-faqs/>)

Ask our Experts



QUESTION 39

UNATTEMPTED

You are building an automated transcription service in which Amazon EC2 worker instances 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

The AWS Simple Storage service is the best option for this scenario. The AWS documentation provides the following information on the Simple Storage service

Amazon S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry

For more information on the Simple Storage Service, please refer to the below link

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

Ask our Experts



QUESTION 40

UNATTEMPTED

You are an AWS Administrator for your company. The company currently has a set of AWS resources hosted in a particular region. You have been requested by your supervisor to create a script which could create duplicate resources in another region incase of a disaster. Which of the below AWS services could help fulfil this requirement.

- ☐ A. AWS Elastic Beanstalk
- ☐ B. AWS SQS
- ☒ C. AWS Cloudformation ✓
- ☐ D. AWS SNS

Explanation :

Answer – C



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

Option A is invalid because this is good to get a certain set of defined resources up and running. But It cannot be used to duplicate infrastructure as code.

Option B is invalid because this is the Simple Queue Service which is used for sending messages.

Option D is invalid because this is the Simple Notification service that is used for sending notifications.

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

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

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

Ask our Experts



QUESTION 41 UNATTEMPTED

What are bastion hosts?

- ☐ A. They are instances in the public subnet which are used as a jump server to resources within other subnets. ✓
- ☐ B. They are instances in the private subnet which are used as a jump server to resources within other subnets.
- ☐ C. They are instances in the public subnet which are used to host web resources that can be accessed by users.
- ☐ D. They are instances in the private subnet which are used to host web resources that can be accessed by users.

Explanation :

Answer – A

As the number of EC2 instances in your AWS environment grows, so too does the number of administrative access points to those instances. Depending on where your administrators connect to your instances from, you may consider enforcing stronger network-based access controls. A best practice in this area is to use a bastion. A bastion is a special purpose server instance that is designed to be the primary access point from the Internet and acts as a proxy to your other EC2 instances. The below picture from the AWS documentation shows the setup of the bastion hosts in a public subnet.



Note

Amazon CloudWatch aggregates the following DynamoDB metrics at one-minute intervals:

- ConditionalCheckFailedRequests
- ConsumedReadCapacityUnits
- ConsumedWriteCapacityUnits
- ReadThrottleEvents
- ReturnedBytes
- ReturnedItemCount
- ReturnedRecordsCount
- SuccessfulRequestLatency
- SystemErrors
- TimeToLiveDeletedItemCount
- ThrottledRequests
- UserErrors
- WriteThrottleEvents

Option B is invalid because bastion hosts need to be in the public subnet

Option C and D are invalid because bastion hosts are not used to host web resources.

For more information on Bastion hosts, please visit the below URL:

<https://aws.amazon.com/blogs/security/controlling-network-access-to-ec2-instances-using-a-bastion-server/> (<https://aws.amazon.com/blogs/security/controlling-network-access-to-ec2-instances-using-a-bastion-server/>)

Ask our Experts



You have several AWS reserved instances in your account. They have been running for some time, but now need to be shutdown since they are no longer required. The data is still required for future purposes. Which of the below possible 2 steps can be taken.

- ☐ A. Convert the instance to on-demand instances
- ☐ B. Sell the instances on the AWS Reserved Instance Marketplace ✓
- ☐ C. Take snapshots of the EBS volumes and terminate the instances ✓
- ☐ D. Convert the instance to spot instances

Explanation :

Answer - B and C

The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances, which vary in term lengths and pricing options. For example, you may want to sell Reserved Instances after moving instances to a new AWS region, changing to a new instance type, ending projects before the term expiration, when your business needs change, or if you have unneeded capacity

For more information on selling instances, please visit the below URL:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>

(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-market-general.html>)

Since the data is still required , its better to take snapshots of the existing volumes and then terminate the instances.

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

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

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

Option A and D are invalid , because you cannot convert Reserved instances to either on-demand instances or Spot Instances.

Ask our Experts



QUESTION 43 UNATTEMPTED

You have an EC2 Instance in a particular region. This EC2 Instance has a preconfigured software running on it. You have been requested to create a disaster recovery solution incase the instance in the region fails. Which of the following is the best solution.

- ☐ A. Create a duplicate EC2 Instance in another AZ. Keep it in the shutdown state. When required , bring it back up.
- ☐ B. Backup the EBS data volume. If the instance fails , bring up a new EC2 instance and attach the volume.
- ☐ C. Store the EC2 data on S3. If the instance fails , bring up a new EC2 instance and restore the data from S3.
- ☐ D. Create an AMI of the EC2 Instance and copy it to another region ✓



Explanation :

Answer - D

You can copy an Amazon Machine Image (AMI) within or across an AWS region using the AWS Management Console, the AWS command line tools or SDKs, or the Amazon EC2 API, all of which support the CopyImage action. You can copy both Amazon EBS-backed AMIs and instance store-backed AMIs. You can copy AMIs with encrypted snapshots and encrypted AMIs.

Copying a source AMI results in an identical but distinct target AMI with its own unique identifier. In the case of an Amazon EBS-backed AMI, each of its backing snapshots is, by default, copied to an identical but distinct target snapshot.

Option A is invalid , because it is a maintenance overhead to maintain another non-running instance

Option B is invalid , because the pre-configured software could have settings on the root volume

Option C is invalid because this is a long and inefficient way to restore a failed instance

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

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

(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html>)

Ask our Experts



QUESTION 44 UNATTEMPTED

You have an EC2 instance located in a subnet in AWS. You have installed a web application on this instance. The security group attached to this instance is shown below

Description	Inbound	Outbound	Tags
<div>Edit</div>			
Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0

The VPC has the following Route table attached to it

<div>Edit</div>			
View: <div>All rules</div>			
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-a97272cc	Active	No

You can SSH into the instance from the internet, but you are not able to access the web server via the web browser. Which of the below steps would resolve the issue?



- ☒ A. Add an HTTP rule to the Security Group ✓
- ☐ B. Remove the SSH rule from the security group
- ☐ C. Add the route 10.0.0.0/16 -> igw-a97272cc to the Route Table
- ☐ D. Add the route 0.0.0.0/0 -> local to the Route Table

Explanation :

Answer – A

You need to add the following security rule so that you can access HTTP traffic to the server. Add the rules to the security group as desired.

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	0.0.0.0/0
HTTP	TCP	80	::/0
SSH	TCP	22	0.0.0.0/0

Option B is invalid because then you will not be able to access the server via SSH

Option C and D are invalid because these routes are not ideal routes to add to the VPC.

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

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)

Ask our Experts



QUESTION 45 UNATTEMPTED

Amazon's Redshift uses which block size for its columnar storage

- ☐ A. 2KB
- ☐ B. 8KB
- ☐ C. 16KB
- ☐ D. 32KB
- ☒ E. 1024KB ✓

Explanation :

Answer - E

Columnar storage for database tables is an important factor in optimizing analytic query performance because it drastically reduces the overall disk I/O requirements and reduces the amount of data you need to load from disk.



Typical database block sizes range from 2 KB to 32 KB. Amazon Redshift uses a block size of 1 MB, which is more efficient and further reduces the number of I/O requests needed to perform any database loading or other operations that are part of query execution.

For more information on Redshift column storage, please visit the below URL:

http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html
(http://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html)

Ask our Experts



QUESTION 46 UNATTEMPTED

You working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security.

- ☐ A. Save the API credentials to your php files.
- ☐ B. Don't save your API credentials. Instead create a role in IAM and assign this role to an EC2 instance when you first create it. ✓
- ☐ C. Save your API credentials in a public Github repository.
- ☐ D. Pass API credentials to the instance using instance userdata.

Explanation :

Answer – B

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

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.

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

<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>)

Ask our Experts



QUESTION 47 UNATTEMPTED



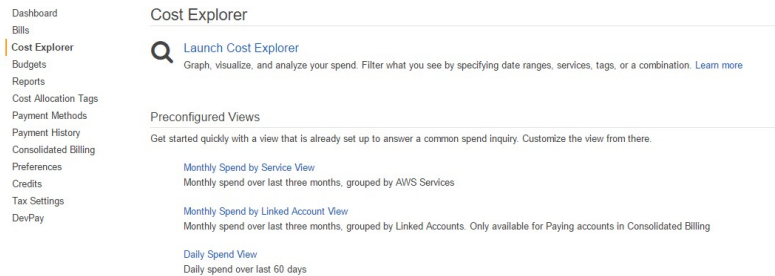
You are a systems administrator and you need to monitor the health of your production environment. You decide to do this using Cloud Watch, however you notice that you cannot see the health of every important metric in the default dashboard. Which of the following metrics do you need to design a custom cloud watch metric for, when monitoring the health of your EC2 instances?

- ☐ A. CPU Usage
- ☒ B. Memory usage ✓
- ☐ C. Disk read operations
- ☐ D. Network in

Explanation :

Answer - B

When you look at your cloudwatch metric dashboard , you can see the metrics for CPU Usage , Disk read operations and Network in



DynamoDB Session Handler

Introduction

The **DynamoDB Session Handler** is a custom session handler for PHP that allows developers to use Amazon DynamoDB as a session store. Using DynamoDB for session storage alleviates issues that occur with session handling in a distributed web application by moving sessions off of the local file system and into a shared location. DynamoDB is fast, scalable, easy to setup, and handles replication of your data automatically.

The DynamoDB Session Handler uses the `session_set_save_handler()` function to hook DynamoDB operations into PHP's native session functions to allow for a true drop in replacement. This includes support for features like session locking and garbage collection which are a part of PHP's default session handler.

For more information on the Amazon DynamoDB service, please visit the [Amazon DynamoDB homepage](#).

You need to add a custom metric for Memory Usage. An example of enabling the custom metric is shown below URL:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html>)

Ask our Experts



QUESTION 48 UNATTEMPTED

In order for an EC2 instance to be accessed from the internet , which of the following are required. Choose 3 answers from the options given below

- ☐ A. An Internet gateway attached to the VPC ✓
- ☐ B. A private IP address attached to the instance



- ☐ C. A public IP address attached to the instance ✓
- ☐ D. A route entry to the Internet gateway in the Route table ✓

Explanation :

Answer - A,C and D

The below image shows the configuration of an instance which can be accessed from the internet. The key requirements are

- 1) An Internet gateway attached to the VPC
- 2) A public IP or elastic IP address attached to the instance
- 3) A route entry to the Internet gateway in the Route table

AssumeRoleWithWebIdentity

Returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider. Example providers include Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider.

Option B is invalid , because this is only required for communication between instances in the VPC.

For more information on Public subnets , please refer to the below URL:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

Ask our Experts



QUESTION 49 UNATTEMPTED

You are using IOT sensors to monitor the number of bags that are handled at an airport. The data gets sent back to a Kinesis stream with default settings. Every alternate day, the data from the stream is sent to S3 for processing. But you notice that S3 is not receiving all of the data that is being sent to the Kinesis stream. What could be the reason for this.



- ☐ A. The sensors probably stopped working on some days hence data is not sent to the stream.
- ☐ B. S3 can only store data for a day
- ☐ C. Data records are only accessible for a default of 24 hours from the time they are added to a stream ✓
- ☐ D. Kinesis streams are not meant to handle IoT related data

Explanation :

Answer – C

Kinesis Streams supports changes to the data record retention period of your stream. An Kinesis stream is an ordered sequence of data records meant to be written to and read from in real-time. Data records are therefore stored in shards in your stream temporarily. The time period from when a record is added to when it is no longer accessible is called the retention period. An Kinesis stream stores records from 24 hours by default, up to 168 hours.

Option A , even though a possibility , cannot be taken for granted as the right option.

Option B is invalid since S3 can store data indefinitely unless you have a lifecycle policy defined.

Option D is invalid because the Kinesis service is perfect for this sort of data injection

For more information on Kinesis data retention , please refer to the below URL:

<http://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html>

(<http://docs.aws.amazon.com/streams/latest/dev/kinesis-extended-retention.html>)

Ask our Experts



QUESTION 50 UNATTEMPTED

A customer wants to track access to their Amazon Simple Storage Service (S3) buckets and also use this information for their internal security and access audits. Which of the following will meet the Customer requirement?

- ☐ A. Enable AWS CloudTrail to audit all Amazon S3 bucket access.
- ☐ B. Enable server access logging for all required Amazon S3 buckets. ✓
- ☐ C. Enable the Requester Pays option to track access via AWS Billing
- ☐ D. Enable Amazon S3 event notifications for Put and Post.

Explanation :

Answer – B

The AWS Documentation mentions the following on S3 Logging

In order to track requests for access to your bucket, you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any. Access log information can be useful in security and access audits.

For more information on the Simple Storage Service logging, please refer to the below link



<http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html>
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html>)

Ask our Experts



QUESTION 51 UNATTEMPTED

You are defined the following Network ACL for your subnet

Edit Save Successful					
View: All rules					
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	Custom TCP Rule	TCP (6)	3000	54.12.34.34/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

What will be the outcome when a workstation of IP 54.12.34.34 tries to access your subnet

- ☐ A. The request will be allowed ✓
- ☐ B. The request will be denied
- ☐ C. The request will be allowed initially and then denied
- ☐ D. The request will be denied initially and then allowed

Explanation :

Answer - A

The following are the parts of a network ACL rule:

Rule number. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it.

Now since the first rule number is 100 and allows all traffic, no matter what rule you put after that all traffic will be allowed. Hence, all options except A are incorrect

For more information on Network ACL, please refer to the below URL:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

Ask our Experts



QUESTION 52 UNATTEMPTED

Which procedure for backing up a relational database on EC2 that is using a set of RAIDed EBS volumes for storage minimizes the time during which the database cannot be written to and results in a consistent backup?

- ☐ A. 1. Detach EBS volumes, 2. Start EBS snapshot of volumes, 3. Re-attach EBS volumes



- ☐ B. 1. Stop the EC2 Instance. 2. Snapshot the EBS volumes
- ☐ C. 1. Suspend disk I/O, 2. Create an image of the EC2 Instance, 3. Resume disk I/O
- ☐ D. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Resume disk I/O
- ☐ E. 1. Suspend disk I/O, 2. Start EBS snapshot of volumes, 3. Wait for snapshots to complete, 4. Resume disk ✓

Explanation :

Answer – E

The AWS Documentation mentions the following when considering snapshot for EBS Volumes in a RAID configuration

When you take a snapshot of an attached Amazon EBS volume that is in use, the snapshot excludes data cached by applications or the operating system. For a single EBS volume, this is often not a problem. However, when cached data is excluded from snapshots of multiple EBS volumes in a RAID array, restoring the volumes from the snapshots can degrade the integrity of the array.

When creating snapshots of EBS volumes that are configured in a RAID array, it is critical that there is no data I/O to or from the volumes when the snapshots are created. RAID arrays introduce data interdependencies and a level of complexity not present in a single EBS volume configuration.

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

<https://aws.amazon.com/premiumsupport/knowledge-center/snapshot-ebs-raid-array/>
(<https://aws.amazon.com/premiumsupport/knowledge-center/snapshot-ebs-raid-array/>)

Ask our Experts



QUESTION 53 UNATTEMPTED

You are a solutions architect working for a company. They store their data on S3, however recently someone accidentally deleted some critical files in S3. You've been asked to prevent this from happening in the future. What options below can prevent this?

- ☐ A. Make sure you provide signed URL's to all users.
- ☐ B. Enable S3 versioning and Multifactor Authentication (MFA) on the bucket. ✓
- ☐ C. Use S3 Infrequently Accessed storage to store the data on.
- ☐ D. Create an IAM bucket policy that disables deletes.

Explanation :

Answer - B

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

You can optionally add another layer of security by configuring a bucket to enable MFA (Multi-Factor Authentication) Delete, which requires additional authentication for either of the following operations.

1) Change the versioning state of your bucket



2) Permanently delete an object version
Option A is invalid because this would be a maintenance overhead
Option C is invalid because changing the storage option will not prevent accidental deletion.
Option D is invalid because the question does not ask to remove the delete permission completely.
For more information on S3 versioning , please refer to the below URL:
<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>)

Ask our Experts



QUESTION 54 UNATTEMPTED

You run an automobile reselling company that has a popular online store on AWS. The application sits behind an Auto Scaling group and requires new instances of the Auto Scaling group to identify their public and private IP addresses. How can you achieve this?

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

Explanation :

Answer – C

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

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

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

Option B is incorrect , because you cannot get the IP address from the cloudwatch metric.

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

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

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>)

Ask our Experts



QUESTION 55 UNATTEMPTED



You are the solution architect for a company. The company has a requirement to deploy an application which will need to have session management in place. Which of the following services can be used to store session data for session management?

- ☐ A. AWS Storage Gateway, ElastiCache & ELB
- ☐ B. ELB, ElastiCache & RDS
- ☐ C. Cloudwatch, RDS & DynamoDB
- ☐ D. RDS, DynamoDB & ElastiCache. ✓

Explanation :

Answer – D

These options are the best when it comes to storing session data.

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 , please visit the below URL:

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

For DynamoDB , this is also evident from the AWS documentation

AWS Lambda Limit Errors

Functions that exceed any of the limits listed in the previous limits tables will fail with an `exceeded limits` exception. These limits are fixed and cannot be changed at this time. For example, if you receive the exception `CodeStorageExceededException` or an error message similar to "Code storage limit exceeded" from AWS Lambda, you need to reduce the size of your code storage.

To reduce the size of your code storage

1. Remove the functions that you no longer use.
2. Reduce the code size of the functions that you do not want to remove. You can find the code size of a Lambda function by using the AWS Lambda console, the AWS Command Line Interface, or AWS SDKs.

For more information , please visit the below URL:

<http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-database.html>

(<http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-database.html>)

And by default , in the industry , RDS have been used to store session data.

The Elastic Load Balancer , AWS Storage Gateway and Cloudwatch cannot store session data.

Ask our Experts



QUESTION 56 UNATTEMPTED

You are working for an Enterprise and have been asked to get a support plan in place from AWS.

- 1) 24x7 access to support
- 2) Access to the full set of Trusted Advisor checks

Which of the following would meet these requirements ensuring that cost is kept at a minimum



- ☐ A. Basic
- ☐ B. Developer
- ☒ C. Business ✓
- ☐ D. Enterprise

Explanation :

Answer - C

Some of the features of Business support are

- 1) 24x7 access to customer service, documentation, whitepapers, and support forums
- 2) Access to full set of Trusted Advisor checks
- 3) 24x7 access to Cloud Support Engineers via email, chat & phone

	Basic	Developer	Business	Enterprise
Customer Service and Communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best Practices	Access to 7 core Trusted Advisor checks	Access to 7 core Trusted Advisor checks	Access to full set of Trusted Advisor checks	Access to full set of Trusted Advisor checks

Option A and B are invalid because they have Access to 6 core Trusted Advisor checks only. And they don't have 24*7 support

Option D is invalid because even though it fulfils all requirements , it is an expensive option and since Business support already covers the requirement , this should be selected , when you are taking cost as an option.

For a full comparison of plans , please visit the following URL:

<https://aws.amazon.com/premiumsupport/compare-plans/>
(<https://aws.amazon.com/premiumsupport/compare-plans/>)

Ask our Experts



QUESTION 57 UNATTEMPTED

Which of the following is incorrect with regards to Private IP addresses?

- ☐ A. In Amazon EC2 classic, the private IP addresses are only returned to Amazon EC2 when the instance is stopped or terminated
- ☐ B. In Amazon VPC, an instance retains its private IP addresses when the instance is stopped.



- ☐ C. In Amazon VPC, an instance does not retain its private IP addresses when the instance is stopped. ✓
- ☐ D. In Amazon EC2 classic, the private IP address is associated exclusively with the instance for its lifetime

Explanation :

Answer - C

The following is true with regards to Private IP addressing.

For instances launched in a VPC, a private IPv4 address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated.

For instances launched in EC2-Classic, we release the private IPv4 address when the instance is stopped or terminated. If you restart your stopped instance, it receives a new private IPv4 address.

For this question you need to choose incorrect with regards to Private IP addresses.

For more information on IP addressing, please refer to the below link:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>
(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>)

Ask our Experts



QUESTION 58 UNATTEMPTED

Which of the following are best practices for monitoring your EC2 Instances

- ☐ A. Create and implement a monitoring plan that collects monitoring data from all of the parts in your AWS solution
- ☐ B. Automate monitoring tasks as much as possible
- ☐ C. Check the log files on your EC2 instances
- ☐ D. All of the above ✓

Explanation :

Answer – D

Use the following best practices for monitoring to help you with your Amazon EC2 monitoring tasks.

- Make monitoring a priority to head off small problems before they become big ones.
- Create and implement a monitoring plan that collects monitoring data from all of the parts in your AWS solution so that you can more easily debug a multi-point failure if one occurs. Your monitoring plan should address, at a minimum, the following questions:
 - What are your goals for monitoring?
 - What resources you will monitor?
 - How often you will monitor these resources?
 - What monitoring tools will you use?
 - Who will perform the monitoring tasks?
 - Who should be notified when something goes wrong?
- Automate monitoring tasks as much as possible.



- Check the log files on your EC2 instances.

For more information on monitoring EC2 , please refer to the below link:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html)

Ask our Experts



QUESTION 59 UNATTEMPTED

For which of the following use cases are Simple Workflow Service (SWF) and Amazon EC2 an appropriate solution? Choose two answers from the options given below

- ☐ A. Using as an endpoint to collect thousands of data points per hour from a distributed fleet of sensors
- ☐ B. Managing a multi-step and multi-decision checkout process of an e-commerce website ✓
- ☐ C. Orchestrating the execution of distributed and auditable business processes ✓
- ☐ D. Using as an SNS (Simple Notification Service) endpoint to trigger execution of video transcoding jobs
- ☐ E. Using as a distributed session store for your web application

Explanation :

Answer- B and C

The AWS Documentation mentions the following on the AWS Simple Workflow service

The Amazon Simple Workflow Service (Amazon SWF) makes it easier to develop asynchronous and distributed applications by providing a programming model and infrastructure for coordinating distributed components and maintaining their execution state in a reliable way. By relying on Amazon SWF, you are freed to focus on building the aspects of your application that differentiate it.

For more information on the simple workflow service, please refer to the below link:

<http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dg-intro-to-swf.html>

(<http://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dg-intro-to-swf.html>)

Ask our Experts



QUESTION 60 UNATTEMPTED

You work for a major news network in Europe. They have just released a new app which allows users to report on events as and when they happen using their mobile phone. Users are able to upload pictures from the app and then other users will be able to view these pics. Your organization expects this app to grow very quickly, essentially doubling it's user base every month. The app uses S3 to store the media and you are expecting sudden and large increases in traffic to S3 when a major news



event takes place as people will be uploading content in huge numbers). You need to keep your storage costs to a minimum however and it does not matter if some objects are lost. Which storage media should you use to keep costs as low as possible?

- ☐ A. S3 – Infrequently Accessed Storage.
- ☒ B. S3 – Reduced Redundancy Storage (RRS). ✓
- ☐ C. Glacier.
- ☐ D. S3 – Provisioned IOPS.

Explanation :

Answer – B

Since the requirement mentions that it does not matter if objects are lost and you need a low cost storage option then Reduced Redundancy Storage is the best option.

The AWS Documentation mentions the below on Reduced Redundancy Storage

Reduced Redundancy Storage (RRS) is an Amazon S3 storage option that enables customers to store noncritical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. It provides a highly available solution for distributing or sharing content that is durably stored elsewhere, or for storing thumbnails, transcoded media, or other processed data that can be easily reproduced

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

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

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14546>)

Certification

- ➦ Cloud Certification
(<https://www.whizlabs.com/cloud-certification-training-courses/>)
- ➦ Java Certification
(<https://www.whizlabs.com/oracle-java-certifications/>)
- ➦ PM Certification
(<https://www.whizlabs.com/project-management-certifications/>)
- ➦ Big Data Certification
(<https://www.whizlabs.com/big-data-certifications/>)

Company

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



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>)

© Copyright 2018. Whizlabs Software Pvt. Ltd. All Rights Reserved.

