(https://www.whizlabs.com/learn) › My Courses (https://www.whizlabs.com/learn/my-courses)
› AWS Certified SysOps Administrator Associate (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests#section-1)
› New Practice Test IV (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14843)
› Report

NEW PRACTICE TEST IV

Attempt	1	**Completed on**	Tuesday , 29 January 2019 , 02:03 PM
Marks Obtained	1 / 65	**Time Taken**	00 H 00 M 47 S
Your score is	1.54%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	65	1	1	63

65	1	1	63
Questions	Correct	Incorrect	Unattempted

Show Answers All ▼

QUESTION 1 INCORRECT

A company has a web application hosted on an EC2 Instance. The application has become a recent target for attacks from the Internet. The attacks are making use of malformed HTTP requests. Which of the following service can help mitigate this attack?

○ **A.** AWS Application Load balancer

○ **B.** AWS Autoscaling

○ **C.** Network Access Control Lists ✖

○ **D.** AWS WAF ✔

Explanation :

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

Option A is incorrect since the Load balancer service is only used to distribute traffic
Option B is incorrect since this service is used to scale the architecture
Option C is incorrect since this feature cannot be used to block application level attacks
For more information on AWS WAF, please refer to the below URL

- https://aws.amazon.com/waf/ (https://aws.amazon.com/waf/)

Ask our Experts

QUESTION 2 CORRECT

A company has a set of files in an S3 bucket. They are worried about all the attacks that happen across the Internet. They are especially worried about cases where data is stolen and subject to ransomware. Which of the following can help protect the files in the bucket?

○ **A.** Enable Versioning on the S3 bucket

○ **B.** Enable S3 Bucket Encryption ✓

○ **C.** Moving the objects to Amazon Glacier

○ **D.** Moving the objects to S3-Infrequent Access

Explanation :

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

· Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

· Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Option A is incorrect since this is used to avoid accidental deletion of objects
Options C and D are incorrect since these are used to move objects to lower cost storage
For more information on using encryption, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html)

Ask our Experts

QUESTION 3 UNATTEMPTED

A company has a set of files in an S3 bucket. Recently some employees inadvertently deleted some files from the bucket. The CIO has now informed you that all measures should be taken to ensure that the objects in the bucket are protected from such sort of incidents in the future. How could this be accomplished?

○ **A.** Enable MFA by using root credentials and by using the AWS CLI ✓

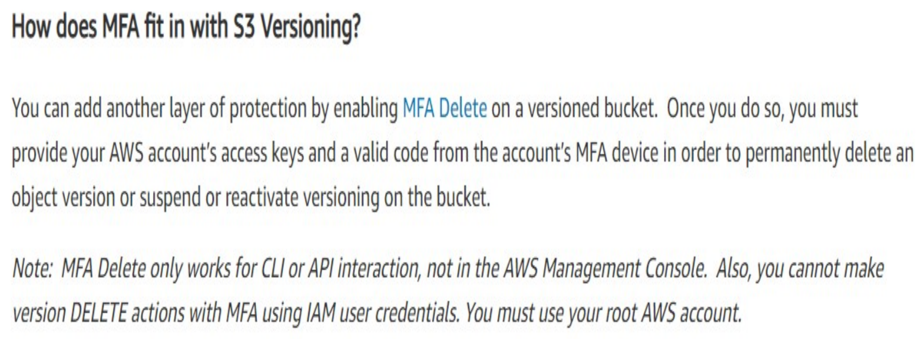
○ **B.** Enable MFA by using root credentials and by using the AWS Console

○ **C.** Enable MFA by using an IAM user with administrative privileges and using the AWS CLI

○ **D.** Enable MFA by using an IAM user with administrative privileges and using the AWS Console.

Explanation :

Answer – A
This is given in the AWS Documentation



How does MFA fit in with S3 Versioning?

You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS account's access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.

Note: MFA Delete only works for CLI or API interaction, not in the AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

Because this is clearly mentioned in the documentation, all other options are invalid

For more information on MFA delete, please refer to the below URL

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

Steps to activate MFA Delete through CLI:
1. **aws s3api list-buckets** --> gives the list of S3 buckets in the account.
2. **aws s3api get-bucket-versioning --bucket <*bucket name*>** --> tells us whether versioning is enabled or not on the bucket.
3. **aws s3api put-bucket-versioning --bucket <*bucket name*> --versioning-configuration Status=Enabled--mfa <*device serial number*>**--> this command enables versioning on the mentioned S3 bucket and also enables MFA delete.
Follow the link on how to work with configuring MFA Delete on S3:

- https://docs.aws.amazon.com/AmazonS3/latest/API/RESTBucketPUTVersioningStatus.html (https://docs.aws.amazon.com/AmazonS3/latest/API/RESTBucketPUTVersioningStatus.html)

Ask our Experts

QUESTION 4 UNATTEMPTED

As a Sysops Administrator, you are uploading files from your data center on to AWS Glacier. The total amount of data in your data center is approximately 70 TB. But when you upload files, you can see the names of the files are not the same as those which have uploaded. For example, you upload a file demo.txt and then in Glacier you can see the archive ID as

"TJgHcrOSfAkV6hdPqOATYfp_0ZaxL1pIBOc02iZ0gDPMr2ig-
nhwd_PafstsdIf6HSrjHnP-3p6LCJClYytFT_CBhT9CwNxbRaM5MetS3I-
GqwxI3Y8QtgbJbhEQPs0mJ3KExample"

What can be done to ensure that you can have the same file in Glacier ensuring minimal impact to cost? Choose 2 answers from the options given below.

□ **A.** Create a PostGreSQL database and have an entry for files names in Glacier against the action file names

□ **B.** Upload the files directly to glacier using the AWS Console

□ **C.** Use the AWS Snowball to upload the files to S3 and then move it to Glacier storage for archival using Lifecycle rules. ✔

□ **D.** Use the AWS Snowball Edge device to upload the files. Here the file names will be the same in Glacier

□ **E.** Upload the files in Amazon S3 Infrequent Access and then use lifecycle policies to move them to Glacier ✔

Explanation :

Answer – C and E
You can upload the files to Amazon S3 either directly or by using a Snowball device. The Lifecycle policies can then be used to transition the storage class of the object to Glacier. So here the file names will be preserved.
Option A is invalid because this would not be a cost effective and easy maintenance option
Option B is invalid because you cannot upload files directly to Glacier
Option D is invalid because the Snowball Edge device would not be a cost effective option
For more information on uploading an archive, please refer to the below URL

- https://docs.aws.amazon.com/amazonglacier/latest/dev/uploading-an-archive.html (https://docs.aws.amazon.com/amazonglacier/latest/dev/uploading-an-archive.html)

Ask our Experts

QUESTION 5 UNATTEMPTED

Your company wants to move a database from their On-premise infrastructure to AWS. This is a MySQL database. They want you as a SysOps Administrator to facilitate this move. They want to ensure this move is as easy as possible. Which of the following service would you choose for hosting the database?

○ **A.** AWS RDS ✓

○ **B.** AWS DynamoDB

○ **C.** AWS Redshift

○ **D.** AWS EMR

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.
One of the database engines supported by this service is MySQL. So this would be the best option.
Option B is invalid because this is a NoSQL database solution
Option C is invalid because this is peta byte storage solution
Option D is invalid because this is a Big data solution
For more information on AWS RDS, please refer to the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html)

Ask our Experts

QUESTION 6 UNATTEMPTED

An application is hosted via a Load Balancer and Autoscaling Group. The application utilizes a lot of memory. Which of the following inbuilt metrics should be used for Autoscaling?

○ **A.** Memory Utilization

○ **B.** CPU Utilization ✓

○ **C.** BackendConnectionErrors

○ **D.** HealthyHostCount

Explanation :

Answer – B
Now this is a tricky question. The question mentions that the application is resource intensive. So, by default we can assume that we could scale the instances in the Autoscaling Group by the Memory utilization. But then it also mentions that we need to use a built-in metric. And Memory is not a built in metric for EC2 in Cloudwatch , so we will use the metric of CPU Utilization
Option A is invalid because this is not an In-built metric
Options C and D are incorrect since these are metrics for the Elastic Load Balancer. And we should scale based on the utilization of the EC2 Instances
For more information on the available metrics for EC2, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html)

Ask our Experts 👍 👎

QUESTION 7 UNATTEMPTED

An application is hosted via a Load Balancer and Autoscaling Group. There are lot of 4xx errors being faced by users. You need to ensure that you understand the client addresses from these errors originated. How can you accomplish this?

○ **A.** If the Elastic Load Balancer logs were enabled, you can use the logs in the Simple Storage service to get the IP addresses. ✓

○ **B.** You can query the client's workstations to get the logs

○ **C.** The logs would automatically be available. Download the logs using the Elastic Load Balancer Console.

○ **D.** Get the logs from the Autoscaling Group

Explanation :

Answer – A
The AWS Documentation mentions the following with the availability of logs for the Elastic Load Balancer
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.
Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify. You can disable access logging at any time.
Option B is invalid since this is not a viable option
Option C is invalid since the ELB logs would be available in S3 and by default are not automatically available
Option D is invalid since we need to get the ELB logs
For more information on ELB access logs, please refer to the below URL

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

Ask our Experts

QUESTION 8 UNATTEMPTED

You’re the SysOps Administrator for a company. You have been instructed to setup a web server and database server in a VPC. The database server should not have connectivity to the Internet. But you need to ensure that the database server can securely download updates from the Internet? Which of the following could you add to the VPC to achieve this? Choose 2 answers from the options given below.

□ **A.** NAT Instance ✓

□ **B.** NAT gateway ✓

□ **C.** VPC Peering

□ **D.** VPN Connection

Explanation :

Answer – A and B

The AWS Documentation mentions the following

You can use a NAT device to enable instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances. A NAT device forwards traffic from the instances in the private subnet to the Internet or other AWS services, and then sends the response back to the instances. When traffic goes to the Internet, the source IPv4 address is replaced with the NAT device’s address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances’ private IPv4 addresses.

AWS offers two kinds of NAT devices—a *NAT gateway* or a *NAT instance*.

Option C is incorrect since this is used to connect multiple VPC’s together

Option D is incorrect since this used to establish virtual private connections

For more information on the NAT device, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat.html (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat.html)

Ask our Experts

QUESTION 9 UNATTEMPTED

A company has a number of sensitive files available in an S3 bucket. The CIO is worried about the security of the documents in the bucket. As the SysOps Administrator, you have been instructed to ensure all objects in the bucket are encrypted at rest. How can you achieve this?

○ **A.** Enable AWS S3 Default Encryption ✔

○ **B.** Place the following statement in the bucket policy "Statement": [{ "Sid": "Stmt1504640908907", "Effect": "Deny", "Principal": "*", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::/*", "Condition": { "Bool": { "aws:SecureTransport": "false" } } }]

○ **C.** Place the following statement in the bucket policy "Statement": [{ "Sid": "Stmt1504640908907", "Effect": "Allow", "Principal": "*", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::/*", "Condition": { "Bool": { "aws:SecureTransport": "false" } } }]

○ **D.** Enable versioning for the buckets

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon S3 default encryption provides a way to set the default encryption behaviour for an S3 bucket. You can set default encryption on a bucket so that all objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS KMS-managed keys (SSE-KMS).
Options B and C are incorrect since this is used for securing data in transit
Option D is incorrect since this is used to help in avoiding accidental deletion of objects
For more information on S3 bucket Encryption, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html)

Ask our Experts 👍 👎

QUESTION 10 UNATTEMPTED

You work as a SysOps Administrator for a company. There is a Security requirement to ensure that API calls for EC2 Instances are logged. You also need to be notified of any Termination API calls for EC2 Instances. How can you automate this requirement? Choose 2 answers from the options given below

☐ **A.** Create a trail in Cloudtrail ✔

☐ **B.** Create a log stream in Cloudwatch

□ **C.** Create a Lambda function and add it as an event destination for the S3 bucket. Use SNS topic for notification. ✔

□ **D.** Create an SNS topic and add it as an event destination for the S3 bucket

Explanation :

Answer – A and C
The AWS Documentation mentions the following
AWS CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. CloudTrail captures API calls as events. For an ongoing record of events in your AWS account, you create a trail. A trail enables CloudTrail to deliver log files of events to an Amazon S3 bucket.
You can take advantage of Amazon S3's bucket notification feature and direct Amazon S3 to publish object-created events to AWS Lambda. Whenever CloudTrail writes logs to your S3 bucket, Amazon S3 can then invoke your Lambda function by passing the Amazon S3 object-created event as a parameter. The S3 event provides information, including the bucket name and key name of the log object that CloudTrail created. Your Lambda function code can read the log object and process the access records logged by CloudTrail. For example, you might write Lambda function code to notify you if specific API call was made in your account.
Option B is incorrect since the correct service for API Logging is Cloudtrail
Option D is incorrect since AWS Lambda functions should be used for notifications
For more information on Lambda with Cloudtrail, please refer to the below URL

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

Ask our Experts

QUESTION 11 UNATTEMPTED

A company has a series of infrastructure stacks which make use of Chef and Puppet recipes which they want to host in AWS. The company wants to ensure that this is done in the easiest way possible. Which of the following service would be ideal for this scenario?

○ **A.** AWS Beanstalk

○ **B.** AWS Opswork ✔

○ **C.** AWS EC2

○ **D.** AWS Config

Explanation :

Answer – B
The AWS Documentation mentions the following

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 (https://aws.amazon.com/ec2/) instances or on-premises compute environments.
Option A is incorrect since this service does not have inbuilt support for Chef and Puppet
Option C is incorrect since this would involve a lot of maintenance
Option D is incorrect since this is a configuration service
For more information on AWS Opswork, please refer to the below URL

- https://aws.amazon.com/opsworks/ (https://aws.amazon.com/opsworks/)

Ask our Experts

QUESTION 12 UNATTEMPTED

A company has an on-premise asymmetric key management service. They want to integrate this with AWS Services. How can you achieve this?

○ **A.** Use AWS KMS and integrate this with the on-premise service

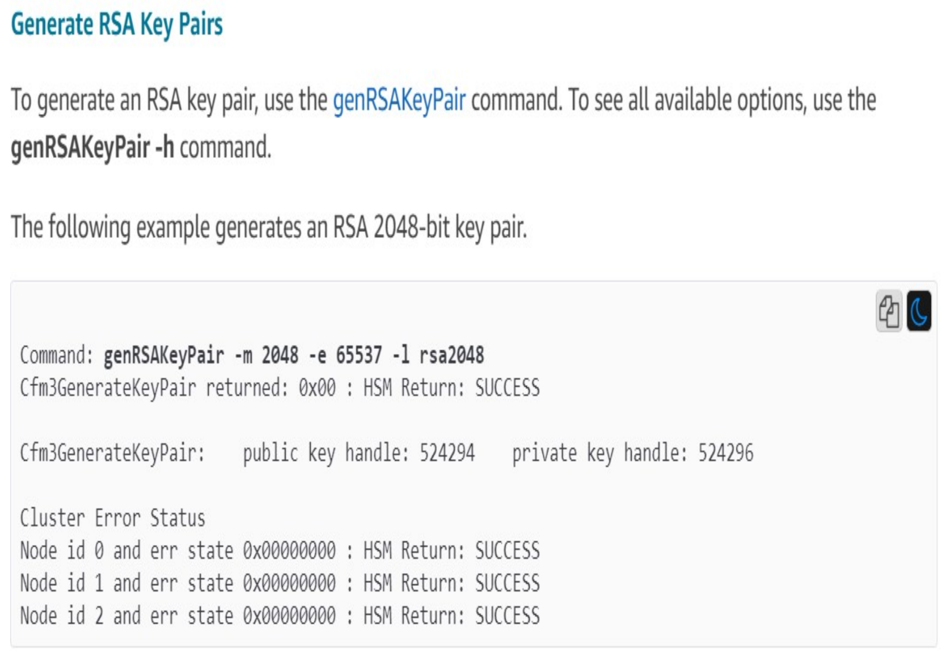
○ **B.** Use AWS CloudHSM and integrate this with the on-premise service ✓

○ **C.** Upload the customer key from KMS to the on-premise service

○ **D.** Create an EC2 Instance out of the AMI from the AWS Marketplace

Explanation :

Answer – B
With CloudHSM you can work with both Symmetric and asymmetric keys
So, the below snapshot from the documentation shows how to generate RSA keys



Generate RSA Key Pairs

To generate an RSA key pair, use the genRSAKeyPair command. To see all available options, use the **genRSAKeyPair -h** command.

The following example generates an RSA 2048-bit key pair.

```
Command: genRSAKeyPair -m 2048 -e 65537 -l rsa2048
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS

Cfm3GenerateKeyPair:    public key handle: 524294    private key handle: 524296

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

Options A and C is incorrect since here you can only generate symmetric keys

Option D is incorrect since you can use the Cloud HSM service for this
For more information on managing keys in HSM, please refer to the below URL

- https://docs.aws.amazon.com/cloudhsm/latest/userguide/manage-keys.html (https://docs.aws.amazon.com/cloudhsm/latest/userguide/manage-keys.html)

Ask our Experts

QUESTION 13 UNATTEMPTED

Your company has setup a company web site by hosting an application on a set of EC2 Instances. They have placed an Elastic Load Balancer in front of the EC2 Instances. You need to point an ELB to the zone apex record(company.com). Which of the following records would you use for this?

○ **A.** TXT

○ **B.** MX

○ **C.** ALIAS ✓

○ **D.** AAA

Explanation :

Answer – C
The AWS Documentation mentions the following

Unlike a CNAME record, you can create an alias record at the top node of a DNS namespace, also known as the *zone apex*. For example, if you register the DNS name example.com, the zone apex is example.com. You can't create a CNAME record for example.com, but you can create an alias record for example.com that routes traffic to www.example.com.

When Route 53 receives a DNS query for an alias record, Route 53 responds with the applicable value for that resource:

· A CloudFront distribution – Route 53 responds with one or more IP addresses for CloudFront edge servers that can serve your content.

· An Elastic Beanstalk environment – Route 53 responds with one or more IP addresses for the environment.

· An ELB load balancer – Route 53 responds with one or more IP addresses for the load balancer.

· An Amazon S3 bucket that is configured as a static website – Route 53 responds with one IP address for the Amazon S3 bucket.

· Another Route 53 record in the same hosted zone – Route 53 responds as if the query is for the record that is referenced by the alias record.

Because of what mentioned in the AWS Documentation , all other options are invalid

For more information on choosing ALIAS records, please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html)

Ask our Experts 👍 👎

QUESTION 14 UNATTEMPTED

You have 2 sets of Instances, one is for the web layer and the other is for the database layer. You need to ensure internal communication for these instances. You have to ensure that the instances cannot communicate with the Internet. Which of the following setups would adhere to this requirement?

○ **A. Private subnets in different availability zones for the web and database layer.** ✔

○ **B. Public subnets in different availability zones for the web and database layer.**

○ **C. Private subnets in different regions for the web and database layer.**

○ **D. Public subnets in different regions for the web and database layer.**

Explanation :

Answer – A

You can have the subnets as private subnets and the Instances can communicate via their private IP addresses

Option B is incorrect since you should not use public subnets since it clearly mentions that the Instances should not be accessible to the Internet

Options C and D are incorrect since the Instances should be in a region and not across regions.

For more information on an example for a VPC configuration, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

Ask our Experts 👍 👎

QUESTION 15 UNATTEMPTED

You have 2 sets of Instances, one is for the web layer and the other is for the database layer. The database server should not be publicly accessible. You have tested the setup, but you can see that the web server cannot access external services. Which of the following can help solve this issue?

○ **A.** Create an Internet gateway, attach it to the VPC. Modify the Route tables for the subnet for the web server. ✓

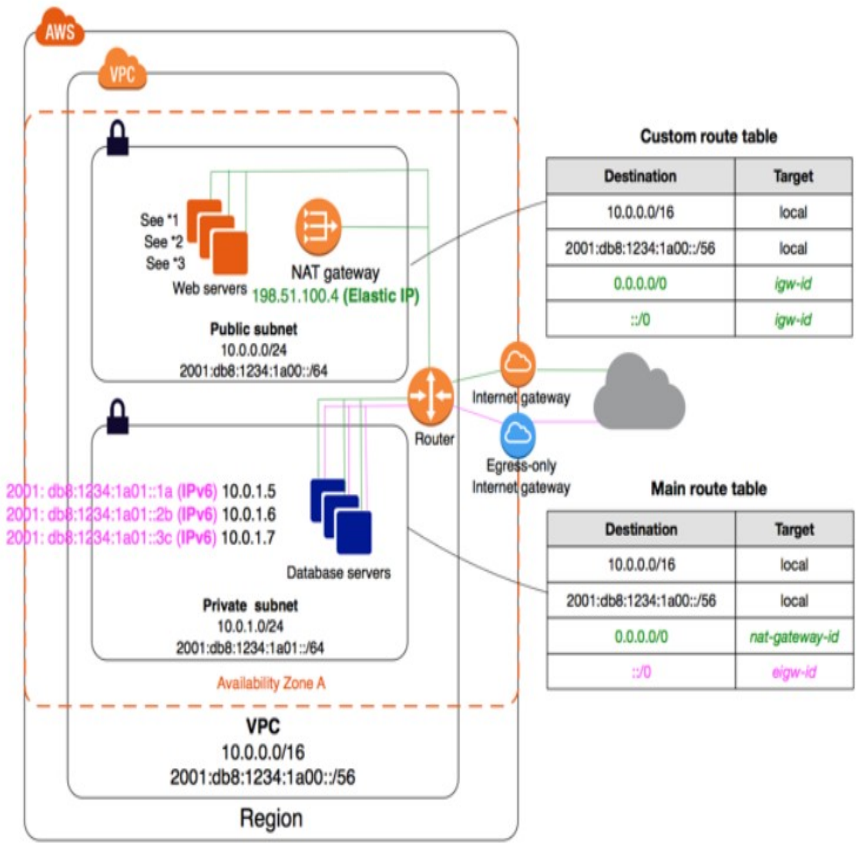
○ **B.** Create a NAT gateway, attach it to the VPC. Modify the Route tables for the subnet for the web server.

○ **C.** Ensure that private IP's are assigned to the web servers for communication

○ **D.** Ensure that the web server is placed behind an Elastic Load Balancer

Explanation :

Answer – A
The below diagram shows an example of a VPC with a public and private subnet. Here the web servers can be placed in the public subnet. Here you need to attach an Internet gateway to the VPC and modify the route tables accordingly.



Custom route table

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	igw-id
::/0	igw-id

Main route table

Destination	Target
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	nat-gateway-id
::/0	eigw-id

Option B is incorrect since the NAT gateway is normally used for secure communication of Instances in the private subnet

Option C is incorrect since private IP's are not used for communication with the Internet
Option D is incorrect since it is not necessary that the Instances need to be placed behind an ELB for Internet access
For more information on an example for a VPC configuration, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

Ask our Experts

QUESTION 16 UNATTEMPTED

You currently have a setup which contains a web server in a private subnet and a bastion host in the public subnet. You have set the following Inbound Rules for the security groups for the Bastion host.

Protocol Type:TCP

Port Number:22

Source:51.10.2.1/32

Protocol Type:TCP

Port Number:22

Source:sg-xxxxxxxx

Protocol Type:TCP

Port Number:389

Source:10.2.1.0/24

Ideally the setup to the bastion host should only connect from the IP address of 51.10.2.1. But from the logs you can see there are other IPs also having the ability to establish a connection to the bastion host? Which of the following is a clear explanation for this?

○ **A.** The source IP of 51.10.2.1/32 does not limit the access to just one IP address

○ **B.** Since you have allowed the connection to port 389 which is higher than port 22, hence other IPs are also able to establish communications.

○ **C.** The IP addresses belonging to the security group of sg-xxxxxxxx are able to connect to the bastion host ✔

○ **D.** By default, all IP addresses are allowed communication into the subnet from the Internet

Explanation :

Answer – C
Since the security group for the bastion host is also allowing communication from the security group for sg-xxxxxxxx , the IP addresses from this security group also have the ability to communicate with the bastion host
Option A is incorrect since the /32 does limit it to one IP address
Options B and D are incorrect since these are not valid points
For more information on security groups for the VPC, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

Ask our Experts 👍 👎

QUESTION 17 UNATTEMPTED

You are a SysOps Administrator for a company. Your company has a set of EC2 Instances in a VPC. You have been told that a report needs to be generated for the list of IP addresses which are establishing communication with the Instances in the subnet. Which of the following can help you achieve this requirement?

○ **A.** AWS VPC Flow Logs ✔

○ **B.** AWS Cloudwatch

○ **C.** AWS Cloudtrail

○ **D.** AWS Config

Explanation :

Answer – A
The AWS Documentation mentions the following
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.
Option B is incorrect since these are just meant for a logging service. Yes you can direct VPC Flow logs to Cloudwatch , but the primary feature which still needs to be used for this requirement is VPC Flow logs
Option C is incorrect since this service is used for API logging
Option D is incorrect since this service is used for configuration management
For more information on VPC Flow logs, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html (https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html)

Ask our Experts

QUESTION 18 UNATTEMPTED

Your company has a set of files in an S3 bucket. The CIO wants to be informed when access to a bucket is open to the world. Which of the following can be used as a security measure but also ensuring that you don’t put too much access restrictions on the bucket for existing users.

○ **A.** Use a bucket policy and place a DENY statement for the PutObject Action

○ **B.** Use AWS Config to monitor any malicious activity and then use SNS to send notifications to the security department ✔

○ **C.** Enable versioning for the bucket

○ **D.** Place the following statement in the bucket policy { "Version":"2012-10-17", "Statement":[{ "Sid":"AddPerm", "Effect":"Allow", "Principal": "*", "Action": ["s3:GetObject"], "Resource":["arn:aws:s3:::examplebucket/*"] }]}

Explanation :

Answer – B
The AWS Documentation mentions the following

AWS Config (https://aws.amazon.com/config) enables continuous monitoring of your AWS resources, making it simple to assess, audit, and record resource configurations and changes. AWS Config does this through the use of rules that define the desired configuration state of your AWS resources. AWS Config provides a number of AWS managed rules (https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html) that address a wide range of security concerns such as checking if you encrypted your Amazon Elastic Block Store (Amazon EBS) volumes, tagged your resources appropriately, and enabled multi-factor authentication (MFA) for root accounts
Option A is incorrect since this will put a restriction on the bucket users
Option C is incorrect since can only prevent from accidental deletion of objects
Option D is incorrect since this puts a security risk for allowing anonymous access to users
For more information on using AWS Config with S3, please refer to the below URL

- https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/ (https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/)

Ask our Experts 👍 👎

QUESTION 19 UNATTEMPTED

You work as a SysOps Administrator for a company. They have a set of EC2 Instances and there is a requirement to monitor the Memory utilization of these resources. How could you go about achieving this?

○ **A.** Use the inbuilt metrics available in Cloudwatch

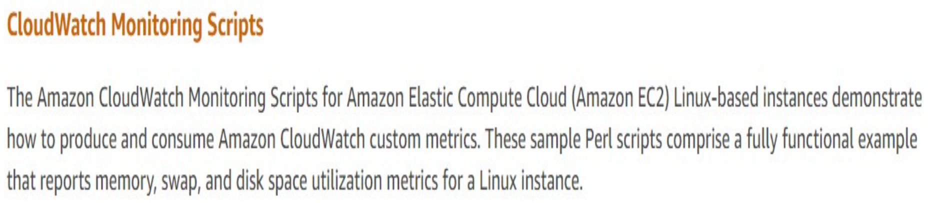
○ **B.** Install scripts on the EC2 Instance to publish custom metrics to CloudWatch ✓

○ **C.** Use the AWS Config service to configure the Memory utilization of the Instance

○ **D.** Use the AWS Inspector service to configure the Memory utilization of the Instance

Explanation :

Answer – B
You need to use custom scripts for monitoring the memory utilization of Instances
The AWS Documentation mentions the following



CloudWatch Monitoring Scripts

The Amazon CloudWatch Monitoring Scripts for Amazon Elastic Compute Cloud (Amazon EC2) Linux-based instances demonstrate how to produce and consume Amazon CloudWatch custom metrics. These sample Perl scripts comprise a fully functional example that reports memory, swap, and disk space utilization metrics for a Linux instance.

Option A is incorrect since there is no inbuilt metrics for Memory utilization

Options C and D are incorrect since these services cannot be used for enabling memory utilization of the instances
For more information on using monitoring scripts, please refer to the below URL

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

Ask our Experts

QUESTION 20 UNATTEMPTED

You work as a SysOps Administrator for a company. The company wants to deploy a MongoDB database which will be heavily used by an application. The database needs to be hosted on an EC2 Instance. You need to provision the environment. Which of the following EBS volume type would you use for the EBS volumes for the underlying Instance?

○ **A.** General Purpose SSD

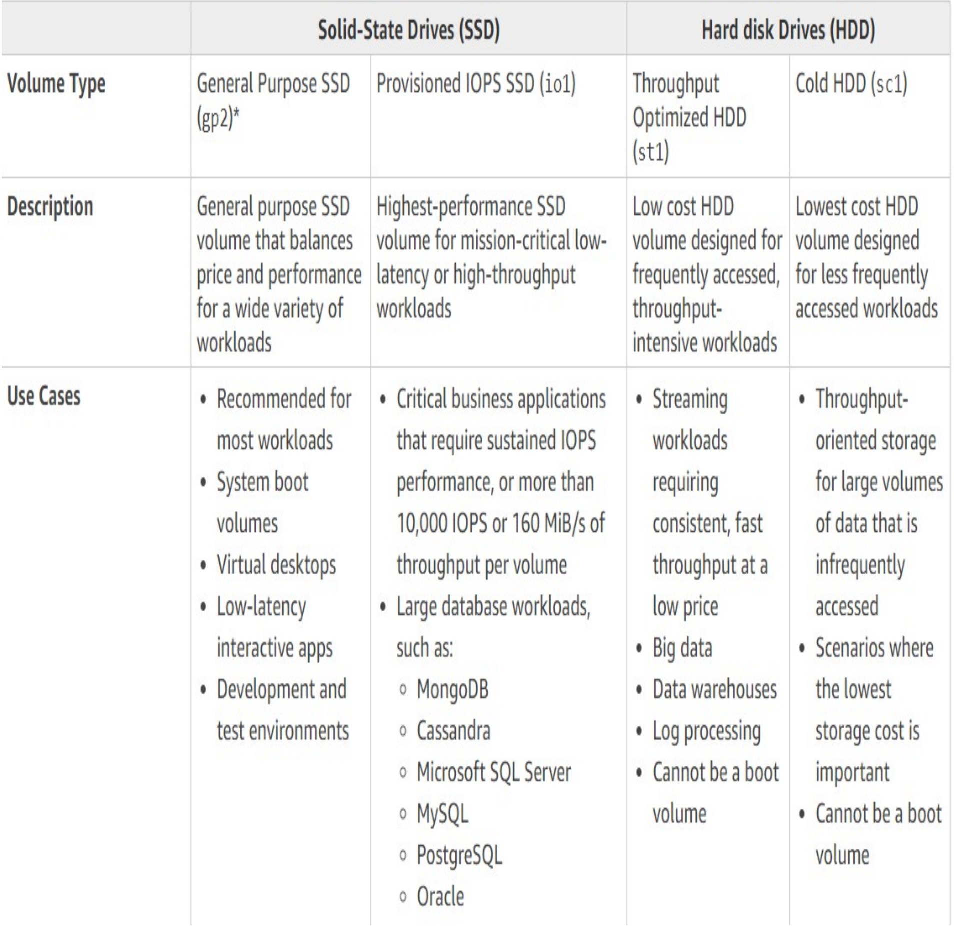
○ **B.** Provisioned IOPS ✓

○ **C.** Throughput Optimized HDD

○ **D.** Cold HDD

Explanation :

Answer – B
The AWS Documentation mentions the following and in this it mentions clearly what should be the volume type to be used



	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• Recommended for most workloads • System boot volumes • Virtual desktops • Low-latency interactive apps • Development and test environments	• Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume • Large database workloads, such as: ○ MongoDB ○ Cassandra ○ Microsoft SQL Server ○ MySQL ○ PostgreSQL ○ Oracle	• Streaming workloads requiring consistent, fast throughput at a low price • Big data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume

For more information on EBS volume types, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html)

Ask our Experts

QUESTION 21 UNATTEMPTED

A company wants to get an aggregate of the CPU utilization of all of their EC2 Instances across multiple regions. How can they achieve this in the easiest way possible with minimal additional costs? Choose 2 answers from the options available.

□ **A.** Create a custom dashboard. Add widgets for each region. Aggregate the CPU utilization for all Instances in a region to each widget. ✓

□ **B.** Create a custom dashboard. Aggregate the CPU utilization for all Instances and add it as a widget to the dashboard.

□ **C.** Ensure basic monitoring is enabled for the Instances

□ **D.** Ensure detailed monitoring is enabled for the Instances ✓

Explanation :

Answer – A and D
You can aggregate the metrics for AWS resources across multiple resources. Amazon CloudWatch cannot aggregate data across Regions. Metrics are completely separate between Regions.
For example, you can aggregate statistics for your EC2 instances that have detailed monitoring enabled. Instances that use basic monitoring are not included. Therefore, you must enable detailed monitoring (at an additional charge), which provides data in 1-minute periods.
Option B is incorrect since aggregation is not possible across all regions
Option C is incorrect since the documentation mentions that you need detailed monitoring
For more information on monitoring and metrics, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GetSingleMetricAllDimensions.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GetSingleMetricAllDimensions.html)

Ask our Experts 👍 👎

QUESTION 22 UNATTEMPTED

You are currently publishing custom metrics using the AWS CLI. You need to view these metrics in Cloudwatch on the dashboard. How can you achieve this?

○ **A.** Create a text widget. Choose the custom metric from the custom namespace for the widget.

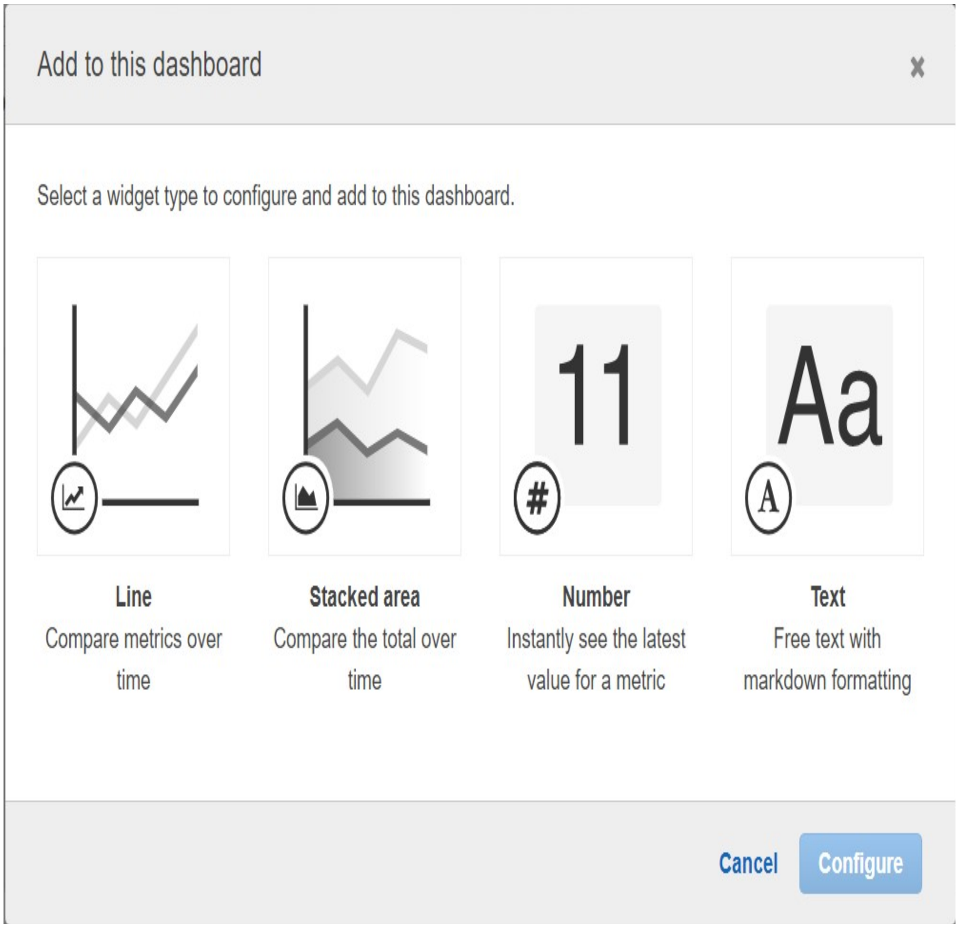
○ **B.** Choose the desired widget. Choose the custom metric from the custom namespace for the widget. ✓

○ **C.** Create a text widget. Choose the inbuilt metric from the custom namespace for the widget.

○ **D.** Choose the desired widget. Choose the inbuilt metric from the custom namespace for the widget.

Explanation :

Answer – B
When you choose a widget for a dashboard, you can choose the widget you want and the custom metric



Add to this dashboard

Select a widget type to configure and add to this dashboard.

Line
Compare metrics over time

Stacked area
Compare the total over time

Number
Instantly see the latest value for a metric

Text
Free text with markdown formatting

Option A is incorrect since this is used when you want a block of text in Markdown (https://docs.aws.amazon.com/general/latest/gr/aws-markdown.html) format.

Options C and D are incorrect since we need to use the custom metrics which we have published
For more information on Cloudwatch dashboards, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html)

Ask our Experts

QUESTION 23 UNATTEMPTED

Your company has a set of EC2 Instances in a VPC. The Security Manager has been informed that a lot of these instances have important security patches that are missing. You need to ensure that these security violations are removed ASAP. Which of the following can help you accomplish this?

○ **A.** AWS Systems Manager ✓

○ **B.** AWS Inspector

○ **C.** AWS Config

○ **D.** AWS Trusted Advisor

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Amazon Linux, and Amazon Linux 2. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option B is incorrect since this can be used to scan instance for vulnerabilities but not patch the instances
Option C is incorrect since this is just a configuration service
Option D is incorrect since this service is only used to give recommendations
For more information on Systems Patch Manager, please refer to the below URL

- https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html)

Ask our Experts 👍 👎

QUESTION 24 UNATTEMPTED

A company is hosting an important revenue generating application. On the last few occasions, the application has come under large DDoS attacks. As a result of this, a lot of users were complaining about the slowness of the application. You need to now avoid these situations in the future and now require 24*7 support from AWS if such situations do occur in the future. Which of the following service can help in this regard?

○ **A.** AWS Shield Advanced ✓

○ **B.** AWS Inspector

○ **C.** AWS WAF

○ **D.** AWS Systems Manager

Explanation :

Answer – A
The AWS Documentation mentions the following

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (https://aws.amazon.com/ec2/) (EC2), Elastic Load Balancing (https://aws.amazon.com/elasticloadbalancing/)(ELB), Amazon CloudFront (https://aws.amazon.com/cloudfront/), and Amazon Route 53 (https://aws.amazon.com/route53/) resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF (https://aws.amazon.com/waf/), a web application firewall. AWS Shield Advanced also gives you 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (https://aws.amazon.com/ec2/) (EC2), Elastic Load Balancing (https://aws.amazon.com/elasticloadbalancing/)(ELB), Amazon CloudFront (https://aws.amazon.com/cloudfront/), and Amazon Route 53 (https://aws.amazon.com/route53/) charges.
Option B is incorrect since this can be used to scan instance for vulnerabilities
Option C is partially correct, you can use the WAF service against certain types of attacks. But for major DDoS attacks, you need to use the AWS Shield Advanced Service
Option D is incorrect since this service cannot protect against DDoS attacks
For more information on AWS Shield service, please refer to the below URL

- https://aws.amazon.com/shield/ (https://aws.amazon.com/shield/)

Ask our Experts 👍 👎

QUESTION 25 UNATTEMPTED

A company is planning on hosting an application that will be installed on a set of EC2 Instances. The application is a batch processing system. The system will be run on weekdays at certain times or even on the weekends. These batch processing workloads basically process data that will then be consumed by business Intelligence applications. Which of the following is the most cost-effective option for the underlying instance provided an occasional interruption in the batch processing is bearable?

○ **A.** Spot Instances ✔

○ **B.** Reserved Instances

○ **C.** Dedicated Hosts

○ **D.** Dedicated Instances

Explanation :

Answer – A
The AWS Documentation mentions the following
A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted

gradually based on the long-term supply of and demand for Spot Instances. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot 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.

The other types of instances would not be cost effective in this situation.

For more information on spot instances, please refer to the below URL

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

Ask our Experts 👍 👎

QUESTION 26 UNATTEMPTED

Your company currently has setup an AWS Direct Connect connection between their on-premise data centre and a VPC in the us-west region. They now want to connect their data centre to a VPC in the us-east region. They need to ensure latency is low and maximum bandwidth for the connection. How could they accomplish this in a cost-effective manner?

○ **A.** Create an AWS Direct Connect connection between the VPC in us-east region and the on-premise data center

○ **B.** Setup an AWS Direct connect gateway ✔

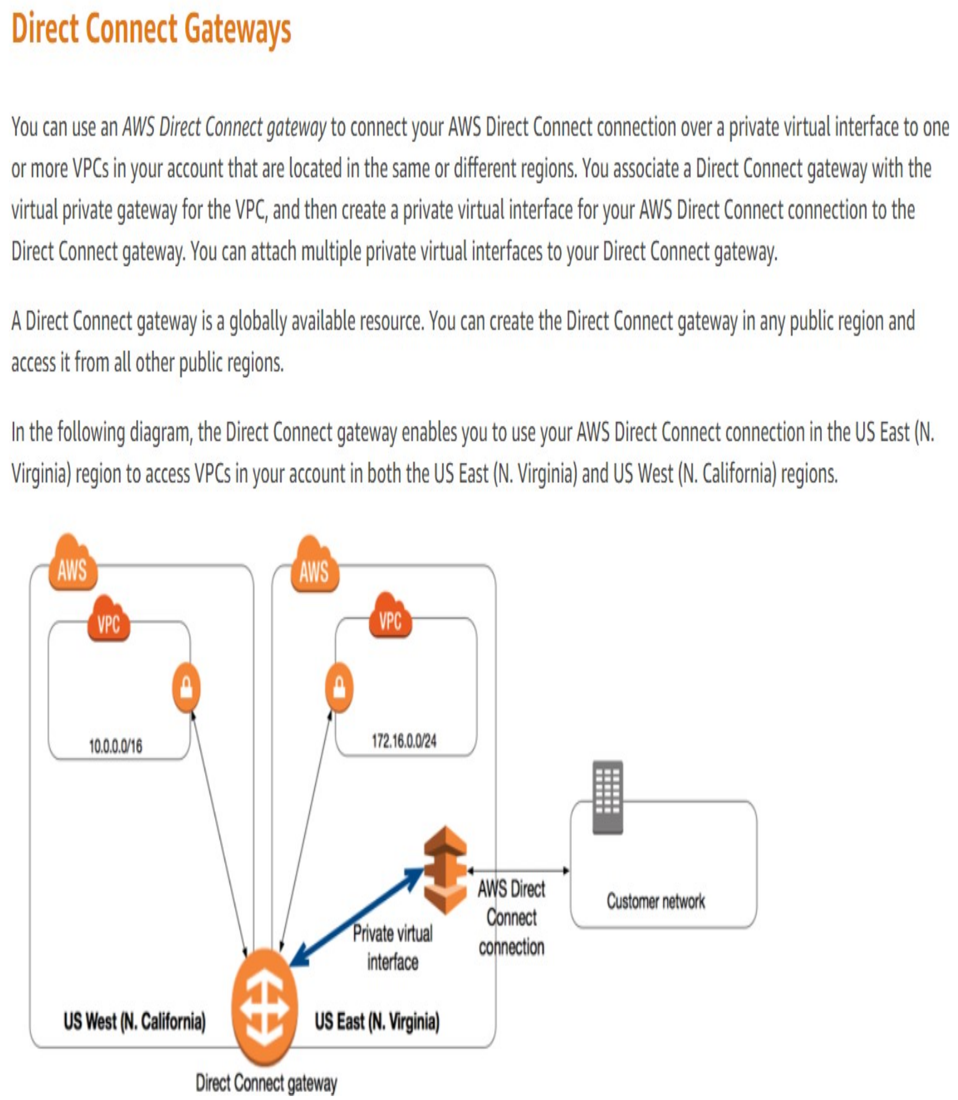
○ **C.** Create an AWS VPN managed connection between the VPC in us-east region and the on-premise data center

○ **D.** Use VPC peering

Explanation :

Answer – B

The AWS Documentation mentions the following



Direct Connect Gateways

You can use an *AWS Direct Connect gateway* to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different regions. You associate a Direct Connect gateway with the virtual private gateway for the VPC, and then create a private virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. You can attach multiple private virtual interfaces to your Direct Connect gateway.

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any public region and access it from all other public regions.

In the following diagram, the Direct Connect gateway enables you to use your AWS Direct Connect connection in the US East (N. Virginia) region to access VPCs in your account in both the US East (N. Virginia) and US West (N. California) regions.

Option A is incorrect since this would add more costs and maintenance

Option C is incorrect since AWS VPN does not lead to a low latency connection
Option D is incorrect since this is used to combine 2 VPC's together
For more information on Direct Connect gateways, please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

Your company has 2 AWS accounts which has individual VPC's. These VPC's need to communicate with each other. The AWS accounts are in different regions. The VPC's have non-overlapping CIDR blocks. Which of the following would be a cost-effective connectivity option?

○ **A.** Use VPN connections

○ **B.** Use VPC peering between the 2 VPC's ✓

○ **C.** Use AWS Direct Connect

○ **D.** Use a NAT gateway

Explanation :

Answer – B
The AWS Documentation mentions the following
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.
AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.
Options A and C are incorrect since VPC peering is easier to establish
Option D is incorrect since this is used for instances in the private subnet to communicate with the Internet
For more information on VPC peering, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html)

Ask our Experts 👍 👎

QUESTION 28 UNATTEMPTED

You've just enabled MFA delete on an S3 bucket. Which of the following actions can you not perform now without using MFA. Choose 2 answers from the options given below

□ **A.** Listing down the deleted versions in the bucket

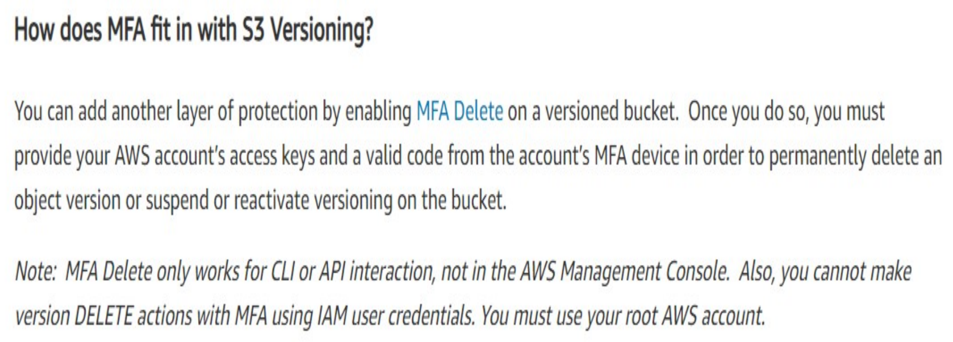
□ **B.** Permanently deleting an object version ✓

□ **C.** Suspend versioning on the bucket ✓

□ **D.** Enable versioning on the bucket

Explanation :

Answer – B and C
The AWS Documentation mentions the following



How does MFA fit in with S3 Versioning?

You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS account's access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.

Note: MFA Delete only works for CLI or API interaction, not in the AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

Because this clearly mentioned in the AWS Documentation, all other options are invalid

For more information on MFA delete, please refer to the below URL

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

Ask our Experts 👍 👎

QUESTION 29 UNATTEMPTED

You've been using Lambda functions to stop EC2 Instances which are not being used frequently. Sometimes the applications on these instances become corrupt as a result of these actions. Which of the following can help to identify these faulty instances?

○ **A.** Resource tagging ✔

○ **B.** CPU utilization

○ **C.** Memory Utilization

○ **D.** Instance Metadata

Explanation :

Answer – A
########
The AWS Documentation mentions the following

"Implement a resource-identification system, such as tags for instances. This helps to ensure that automated actions are targeted to the correct resource, and also allows for easier filtering, modification, and troubleshooting according to categories that you define."
########
For more information refer below URL:
https://aws.amazon.com/answers/infrastructure-management/instance-scheduler/
(https://aws.amazon.com/answers/infrastructure-management/instance-scheduler/)

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags you've assigned to it. For example, you could define a set of tags for your account's Amazon EC2 instances that help you track each instance's owner and stack level.
All other options are invalid since tags are the best way to identify these faulty resources
For more information on resource tagging, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

Ask our Experts 👍 👎

QUESTION 30 UNATTEMPTED

You have a set of EC2 Instances. Sometimes these EC2 Instances reach 100% CPU utilization and need to be restarted. You need to automate this ensuring that the restart happens if the threshold is reached after 2 minutes. How can you accomplish this? Choose 2 answers from the options given below

□ **A.** Use basic monitoring for the instances.

□ **B.** Use Cloudwatch alarms based on the CPU Utilization. Choose the action to restart the instance ✔

□ **C.** Use Detailed monitoring for the instances. ✔

□ **D.** Use Cloudtrail events to restart the instances

Explanation :

Answer – B and C
The AWS Documentation mentions the following
By default, Amazon EC2 sends metric data to CloudWatch in 5-minute periods. To send metric data for your instance to CloudWatch in 1-minute periods, you can enable detailed monitoring on the instance
Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.
Option A is invalid because you need to enable detailed monitoring for the 2-minute interval requirement
Option D is invalid because this is used API monitoring
For more information on using alarm actions, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/UsingAlarmActions.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/UsingAlarmActions.html)

Ask our Experts

QUESTION 31 UNATTEMPTED

Your company owns a set of consulting companies. Each of these company's along with you need to have AWS accounts in place. You need to manage the global permissions and billing for these accounts. Which of the following approach would you consider for this requirement?

○ **A.** Use AWS Organizations ✓

○ **B.** Use IAM policies

○ **C.** Use IAM users

○ **D.** Use Consolidated billing

Explanation :

Answer – A
The AWS Documentation mentions the following
AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes.
Using AWS Organizations, you can create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts. You can also use Organizations to help automate the creation of new accounts through APIs. Organizations helps simplify the billing for multiple accounts by enabling you to setup a single payment method for all the accounts in your organization through consolidated billing. AWS Organizations is available to all AWS customers at no additional charge.
Options B and C are incorrect since these are fine for individual accounts but not for merged accounts
Option D is partially correct, you should now use the complete and new feature of AWS Organizations
For more information on AWS Organizations, please refer to the below URL

- https://aws.amazon.com/organizations/ (https://aws.amazon.com/organizations/)

Ask our Experts

QUESTION 32 UNATTEMPTED

You're a SysOps Administrator for a company. Your CIO wants to ensure that security practises are put in place when it comes to maintaining their infrastructure in AWS. Which of the following would fall under the responsibility of the customer? Choose 2 answers from the options below

□ **A.** Patching of the OS on an EC2 Instance ✓

□ **B.** Rotation of Access Keys for IAM Users ✔

□ **C.** Patching of the OS on the database Instance for AWS RDS

□ **D.** Patching of the database software on AWS RDS

□ **E.** Patching of PHP on an AWS Managed Elastic Beanstalk Application

Explanation :

Answer – A and B
The AWS Documentation mentions the following when it comes the other options
With managed platform updates, you no longer have to worry about keeping up with new patches or updates for the platform running your application. Elastic Beanstalk performs updates in a safe manner so that your end users are minimally impacted. The updates use an immutable deployment (https://aws.amazon.com/about-aws/whats-new/2016/04/aws-elastic-beanstalk-adds-two-new-deployment-policies-and-amazon-linux-ami-2016-03-update/) mechanism. This ensures that Elastic Beanstalk provisions a parallel fleet of Amazon EC2 instances with the updates installed before swapping out and terminating the existing instances. Elastic Beanstalk redirects traffic to the existing fleet of instances if the Elastic Beanstalk health system detects any issues during the update, ensuring minimal impact to end users of your application.
Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying operating system (OS) or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.
For more information on Managed platforms for Elastic Beanstalk and Maintaining the RDS Instance, please refer to the below URL

- https://aws.amazon.com/about-aws/whats-new/2016/04/aws-elastic-beanstalk-introduces-managed-platform-updates/ (https://aws.amazon.com/about-aws/whats-new/2016/04/aws-elastic-beanstalk-introduces-managed-platform-updates/)
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html)

Ask our Experts 👍 👎

QUESTION 33 UNATTEMPTED

A company has an application that needs to be deployed on a set of EC2 Instance. The application needs a lot of dependent files that need to be downloaded and installed. You need ensure that the application is available in the least time possible on another EC2 Instance. Which of the following can help accomplish this?

○ **A.** Create an AMI with the application and the necessary library files ✔

○ **B.** Use the User Data section to install the application and the necessary library files

○ **C.** Create an Opswork stack and ensure the stack downloads the necessary application and files

○ **D.** Create an Elastic Beanstalk environment and ensure the stack downloads the necessary application and files

Explanation :

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

- A template for the root volume for the instance (for example, an operating system, an application server, and applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it's launched

All other options are invalid since all of these would take more time to provision the environment
For more information on AMI's please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AMIs.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AMIs.html)

Ask our Experts

QUESTION 34 UNATTEMPTED

A company has an application that is used to distribute software patches. The application is hosted on a set of EC2 Instance. Users download patch updates. The users are complaining of slow response. Which of the following can be used as an efficient and cost effective option to mitigate this issue?

○ **A.** Use a Cloud front distribution ✓

○ **B.** Use an Application Elastic Load Balancer

○ **C.** Use Route 53

○ **D.** Use a Classic Elastic Load Balancer

Explanation :

Answer – A
The AWS Documentation mentions the following

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.
Options B and D are incorrect since this is only used to distribute traffic
Option C is incorrect since this is a domain name system service
For more information on Cloudfront distributions please refer to the below URL

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

Ask our Experts 👍 👎

QUESTION 35 UNATTEMPTED

Your team has an EC2 Instance which has a volume type of General Purpose SSD. The size of the volume is 5 TB. You need to increase the IOPS on the volume. How can you accomplish this? Choose 2 answers from the options given below

□ **A.** Change the Volume to Provisioned IOPS ✓

□ **B.** Increase the size of the volume

□ **C.** Place the volume in a RAID 0 configuration ✓

□ **D.** Place the volume in a RAID 1 configuration

Explanation :

Answer – A and C
The AWS Documentation mentions the following
An io1 volume can range in size from 4 GiB to 16 TiB and you can provision 100 up to 32,000 IOPS per volume. The maximum IOPS for a General Purpose SSD is 16,000.
For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together.
Option B is incorrect since the maximum IOPS for a general purpose SSD is reached at the size of 5,334 GiB and above
Option D is incorrect since you need to use RAID O
For more information on EBS volume types, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html)
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2 (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2)

Ask our Experts 👍 👎

QUESTION 36 UNATTEMPTED

You're company has a set of EC2 Instance. You have noticed that the Instance CPU credits go down to 0 several times during the monitoring of these instances. Which of the following can help alleviate this? Choose 2 answers from the options given below.

□ **A.** Change to t2.unlimited ✓

□ **B.** Change to a higher instance type ✓

□ **C.** Use t1.micro instances

□ **D.** Use EBS optimized instances

Explanation :

Answer – A and B
The AWS Documentation mentions the following
A burstable performance instance configured as unlimited, such as T3 Unlimited or T2 Unlimited, can sustain high CPU performance for any period of time whenever required. The hourly T3 or T2 instance price automatically covers all interim spikes in usage if the average CPU utilization of the instance is at or below the baseline over a rolling 24-hour period or the instance lifetime, whichever is shorter. If the instance runs at higher CPU utilization for a prolonged period, it can do so for a flat additional rate per vCPU-hour
You can also choose a higher instance type.
Option C is incorrect since this will give less CPU burst credits
Option D is incorrect since this will not ensure high burst credits for CPU's
For more information on burstable performance instances, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-unlimited-mode.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-unlimited-mode.html)

Ask our Experts 👍 👎

QUESTION 37 UNATTEMPTED

Your company wants to migrate a JSON based data store onto AWS. They need low latency data access to the store. The store also needs to be highly available. Which of the following would be the ideal data store in AWS?

○ **A.** AWS Aurora

○ **B.** AWS S3

○ **C.** AWS DynamoDB ✓

○ **D.** AWS Redshift

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling
Option A is incorrect since this is better for SQL based solutions
Option B is incorrect since this is used for object level storage
Option D is incorrect since this is used for data warehousing solutions
For more information on AWS DynamoDB, please refer to the below URL

- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)

Ask our Experts 👍 👎

QUESTION 38 UNATTEMPTED

Your company has a high number of resources hosted in their AWS account. After a recent internal technical audit on the EC2 Instances, it’s been noticed that a lot of Elastic IP’s are not being used. Which of the following can be used to give more cost improvements suggestions?

○ **A.** AWS Trusted Advisor ✓

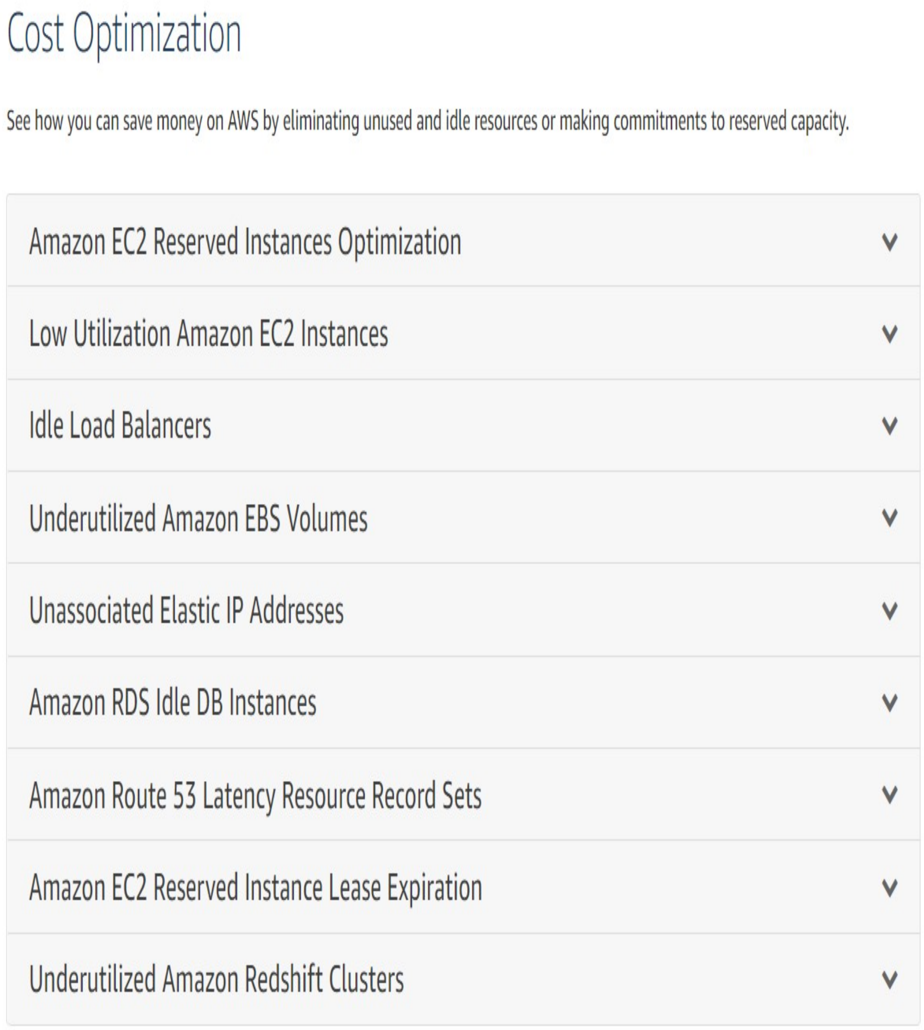
○ **B.** AWS Config

○ **C.** AWS Inspector

○ **D.** AWS Systems Manager

Explanation :

Answer – A
This is one of the major components of the AWS Trusted Advisor



Cost Optimization

See how you can save money on AWS by eliminating unused and idle resources or making commitments to reserved capacity.

Amazon EC2 Reserved Instances Optimization
Low Utilization Amazon EC2 Instances
Idle Load Balancers
Underutilized Amazon EBS Volumes
Unassociated Elastic IP Addresses
Amazon RDS Idle DB Instances
Amazon Route 53 Latency Resource Record Sets
Amazon EC2 Reserved Instance Lease Expiration
Underutilized Amazon Redshift Clusters

Option B is incorrect since this is a configuration-based service

Option C is incorrect since is used to scan servers for vulnerabilities
Option D is incorrect since this is used for managing systems
For more information on AWS Trusted Advisor, please refer to the below URL

- https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/ (https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/)

Ask our Experts

QUESTION 39 UNATTEMPTED

Your company currently has an EC2 Instance in a subnet in one availability zone. You need to ensure scalability and high availability of the application. Which of the following can help achieve this?

○ **A.** Create an Autoscaling Group with subnets across 2 availability zones. Set a minimum, desired and maximum capacity as 1

○ **B.** Create an Autoscaling Group with subnets across 3 availability zones. Set a minimum, desired and maximum capacity as 2 ✓

○ **C.** Create an Autoscaling Group with subnets across 2 regions. Set a minimum, desired and maximum capacity as 1

○ **D.** Create an Autoscaling Group with subnets across 3 regions. Set a minimum, desired and maximum capacity as 2

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon EC2 Auto Scaling enables you to take advantage of the safety and reliability of geographic redundancy by spanning Auto Scaling groups across multiple Availability Zones within a region. When one Availability Zone becomes unhealthy or unavailable, Auto Scaling launches new instances in an unaffected Availability Zone. When the unhealthy Availability Zone returns to a healthy state, Auto Scaling automatically redistributes the application instances evenly across all of the designated Availability Zones.
Option A is incorrect since you only have a capacity of one which does not full comply with scalability and high availability
Options C and D are incorrect since the scaling should happen within a region
For more information on the benefits of Autoscaling, please refer to the below URL

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html)

Ask our Experts 👍 👎

QUESTION 40 UNATTEMPTED

You have Instances being setup as part of an Autoscaling Group. You notice that the new instances are not being part of the aggregated metrics? Which of the following could be a possible reason for this?

○ **A.** It's because the warm period has not expired ✓

○ **B.** It's because the Instances have not completed their boot sequence

○ **C.** It's because the Instances have not been attached to the Autoscaling Group

○ **D.** It's because the wrong launch configuration has been used

Explanation :

Answer – A
The AWS Documentation mentions the following

With step scaling policies, you can specify the number of seconds that it takes for a newly launched instance to warm up. Until its specified warm-up time has expired, an instance is not counted toward the aggregated metrics of the Auto Scaling group. While scaling out, AWS also does not consider instances that are warming up as part of the current capacity of the group. Therefore, multiple alarm breaches that fall in the range of the same step adjustment result in a single scaling activity. This ensures that we don't add more instances than you need.
Since this is clearly given in the AWS Documentation, all other options are invalid
For more information on step scaling policy, please refer to the below URL

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html#as-step-scaling-warmup (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html#as-step-scaling-warmup)

Ask our Experts

QUESTION 41 UNATTEMPTED

Your company has the following architecture for their application on AWS

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend using AWS RDS
- A Load balancer for distribution of traffic
- A NAT gateway for routing traffic from the database server to the Internet

Which of the following can be used to increase the scalability and availability of the application? Choose 2 answers from the options given below

□ **A.** Launch the EC2 Instances as part of an Autoscaling Group ✓

□ **B.** Enable Multi-AZ for the database ✓

□ **C.** Use a NAT Instance instead of a NAT gateway

□ **D.** Use Route 53 instead of the Load balancer

Explanation :

Answer – A and B
The AWS Documentation mentions the following

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called *Auto Scaling groups*. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size.
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).
Option C is incorrect since the NAT gateway is preferred for better scalability and availability
Option D is incorrect since the Load balancer should be used for distributing traffic
For more information on EC2 Autoscaling and RDS Multi-AZ, please refer to the below URL

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html)
- https://aws.amazon.com/rds/details/multi-az/ (https://aws.amazon.com/rds/details/multi-az/)

Ask our Experts 👍 👎

QUESTION 42 UNATTEMPTED

Your company has an AWS account. An external audit is going to be conducted for your account. You need to give an auditor access to the logs so that they can carry out the audit process accordingly. Which of the following is the best way to give access to the auditor?

○ **A.** Create an IAM Role for the auditor. Ask the user to use federated access.

○ **B.** Create an IAM user that has read access to the logs created in S3 by Cloudtrail ✔

○ **C.** Create Access Keys. Give the Access Keys to auditor.

○ **D.** Create an IAM user that has read and write access to the logs created in S3 by Cloudtrail

Explanation :

Answer – B
The AWS Documentation mentions the following
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
Option A is incorrect since federated access is not the ideal access mechanism that should be granted
Option C is incorrect since Access keys is not a secure way to give access
Option D is incorrect since you should not give write access.

For more information on Cloudtrail, please refer to the below URL

- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

Ask our Experts

QUESTION 43 UNATTEMPTED

In your company a team is developing a mobile application. The users for the mobile application need to have the ability to log in and access resources in AWS. Which of the following services would you use? Choose 2 answers from the options given below

□ **A.** AWS Cognito ✓

□ **B.** AWS IAM Roles ✓

□ **C.** AWS Federated Access

□ **D.** AWS IAM users

Explanation :

Answer – A and B
The AWS Documentation mentions the following
Amazon Cognito identity pools assign your authenticated users a set of temporary, limited privilege credentials to access your AWS resources. The permissions for each user are controlled through IAM roles (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html) that you create. You can define rules to choose the role for each user based on claims in the user's ID token. You can define a default role for authenticated users. You can also define a separate IAM role with limited permissions for guest users who are not authenticated.
Since this is clearly mentioned in the documentation, all other options are invalid
For more information on AWS Cognito and IAM Roles, please refer to the below URL

- https://docs.aws.amazon.com/cognito/latest/developerguide/role-based-access-control.html (https://docs.aws.amazon.com/cognito/latest/developerguide/role-based-access-control.html)

Ask our Experts

QUESTION 44 UNATTEMPTED

Your team has just created an AMI out of an EC2 Instance. You need to share it with another account. The account belongs to the same company. Which of the following is the right way to ensure the other account has access the AMI?

○ **A.** Share the AMI with the specific AWS account ✓

○ **B.** Mark the AMI as public

○ **C.** Sell the AMI in the AWS Marketplace

○ **D.** Make the AMI as a paid AMI

Explanation :

Answer – A
The AWS Documentation mentions the following
You can share an AMI with specific AWS accounts without making the AMI public. All you need are the AWS account IDs.
AMIs are a regional resource. Therefore, sharing an AMI makes it available in that region. To make an AMI available in a different region, copy the AMI to the region and then share it.
All of the other options are not valid since these are not secure ways to share the AMI
For more information on sharing the AMI, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html)

Ask our Experts 👍 👎

QUESTION 45 UNATTEMPTED

You work as a SysOps Administrator for a company. You have been requested to create a set of EC2 Instances. While launching the instances you are getting the following error

“InsufficientInstanceCapacity”

Which of the following would you most likely do in this situation? Choose 2 answers from the options given below.

□ **A.** Wait a few minutes and then submit your request again ✓

□ **B.** Try launching an instance with a lower instance type ✓

□ **C.** You have reached the limit on the number of instances that you can launch in a region so raise a request with AWS

□ **D.** You've reached your EBS volume limit so raise a request with AWS

Explanation :

Answer – A and B
Option C is invalid because you should do this when you get the InstanceLimitExceeded error
Option D is invalid since this happens if your instance terminates immediately after launch
The AWS Documentation mentions the following

If you get an InsufficientInstanceCapacity error when you try to launch an instance or restart a stopped instance, AWS does not currently have enough available On-Demand capacity to service your request.
To resolve the issue, try the following:

- Wait a few minutes and then submit your request again; capacity can shift frequently.
- Submit a new request with a reduced number of instances. For example, if you're making a single request to launch 15 instances, try making 3 requests for 5 instances, or 15 requests for 1 instance instead.
- If you're launching an instance, submit a new request without specifying an Availability Zone.
- If you're launching an instance, submit a new request using a different instance type (which you can resize at a later stage).
- If you are launching instances into a cluster placement group, you can get an insufficient capacity error.
- Try purchasing Reserved Instances, which are a long-term capacity reservation.

For more information on troubleshooting the launch of EC2 Instances, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html)

Ask our Experts 👍 👎

QUESTION 46 UNATTEMPTED

You've setup an RDS Instance. An application is being hosted on an EC2 Instance that connects to the AWS RDS Instance. From the application, the following error is being encountered

"Error connecting to database"

You've verified that you are able to connect to the database from a bastion host in a public subnet via the AWS Console. Which of the following could be possible issues? Choose 2 answers from the options given below.

□ **A.** The application is using the wrong port number in the connection string ✓

□ **B.** The database server has the wrong ingress Security group rule for the web server ✓

□ **C.** The database server has the wrong egress Security group rule for the web server

□ **D.** The certificate used by the web server is not recognised by the database server

Explanation :

Answer – A and B
The AWS Documentation mentions the following
When you cannot connect to a DB instance, the following are common causes:

· The access rules enforced by your local firewall and the ingress IP addresses that you authorized to access your DB instance in the instance's security group are not in sync. The problem is most likely the ingress rules in your security group. By default, DB instances do not allow access; access is granted through a security group. To grant access, you must create your own security group with specific ingress and egress rules for your situation.

· The port you specified when you created the DB instance cannot be used to send or receive communications due to your local firewall restrictions. In this case, check with your network administrator to determine if your network allows the specified port to be used for inbound and outbound communication.

· Your DB instance is still being created and is not yet available. Depending on the size of your DB instance, it can take up to 20 minutes before an instance is available.

Since this is clearly given in the AWS Documentation , all other options are incorrect
For more information on troubleshooting connecting to AWS RDS, please refer to the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html#CHAP_Troubleshooting.C
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html#CHAP_Troubleshooting.Co

Ask our Experts 👍 👎

QUESTION 47 UNATTEMPTED

You work as a SysOps Administrator for your company. The company is creating a series of EBS Snapshots. This is required in case there is need to recover an EBS Volume. But as per the business continuity process of the company, EBS snapshots older than 6 months are no longer required. You need to ensure that the snapshots are deleted when not required. How can you do this in the easiest way possible?

○ **A.** Use AWS Lambda functions. Set a scheduled job to execute the Lambda function every 6 months.

○ **B.** Create an EC2 Instance. Setup a cron job to delete EBS snapshots older than 6 months

○ **C.** Use Step Functions and Cloudwatch events to schedule the deletion of older EBS snapshots ✔

○ **D.** Create an Elastic beanstalk environment. Setup a cron job to delete EBS snapshots older than 6 months

Explanation :

Answer - C
The AWS Documentation mentions the following

You can run CloudWatch Events rules according to a schedule. In this tutorial, you create an automated snapshot of an existing Amazon Elastic Block Store (Amazon EBS) volume on a schedule. You can choose a fixed rate to create a snapshot every few minutes or use a cron expression to specify that the snapshot is made at a specific time of day.
Now other options are also viable, but would just result in a maintenance overhead.
For more information on using events for EBS snapshots, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/TakeScheduledSnapshot.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/TakeScheduledSnapshot.html)
- https://aws.amazon.com/blogs/compute/automating-amazon-ebs-snapshot-management-with-aws-step-functions-and-amazon-cloudwatch-events/ (https://aws.amazon.com/blogs/compute/automating-amazon-ebs-snapshot-management-with-aws-step-functions-and-amazon-cloudwatch-events/)

Ask our Experts 👍 👎

QUESTION 48 UNATTEMPTED

Your company currently has an environment that consists of EC2 Instances, S3 buckets , PostGreSQL and the usage of the EFS File system. The IT Security department has now mandated that all data is encrypted at rest. For which of the following can encryption be enabled without causing an interruption to its current usage by users?

○ **A.** EBS volumes

○ **B.** PostGreSQL

○ **C.** S3 buckets ✔

○ **D.** EFS

Explanation :

Answer – C
The AWS Documentation mentions the following
You have the following options of protecting data at rest in Amazon S3.
· Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
· Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

All other options are incorrect because of the following reasons
· The Encryption can not be enabled after the service is created. The encryption is only available when you create the service
· So for example for EBS volumes, PostgreSQL database and EFS , you will need to recreate them and enable encryption during the creation time. This will cause a disruption to users.
For more information on using encryption for S3, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html)

Ask our Experts

QUESTION 49 UNATTEMPTED

Your company has been managing their tapes via a custom vendor solution. There was an incident where the tapes were not available. The company now wants to make use of AWS to stop this solution from occurring in the future. Which of the following would be an ideal solution to help in this regard?

○ **A.** Store all the tape data in Amazon Glacier

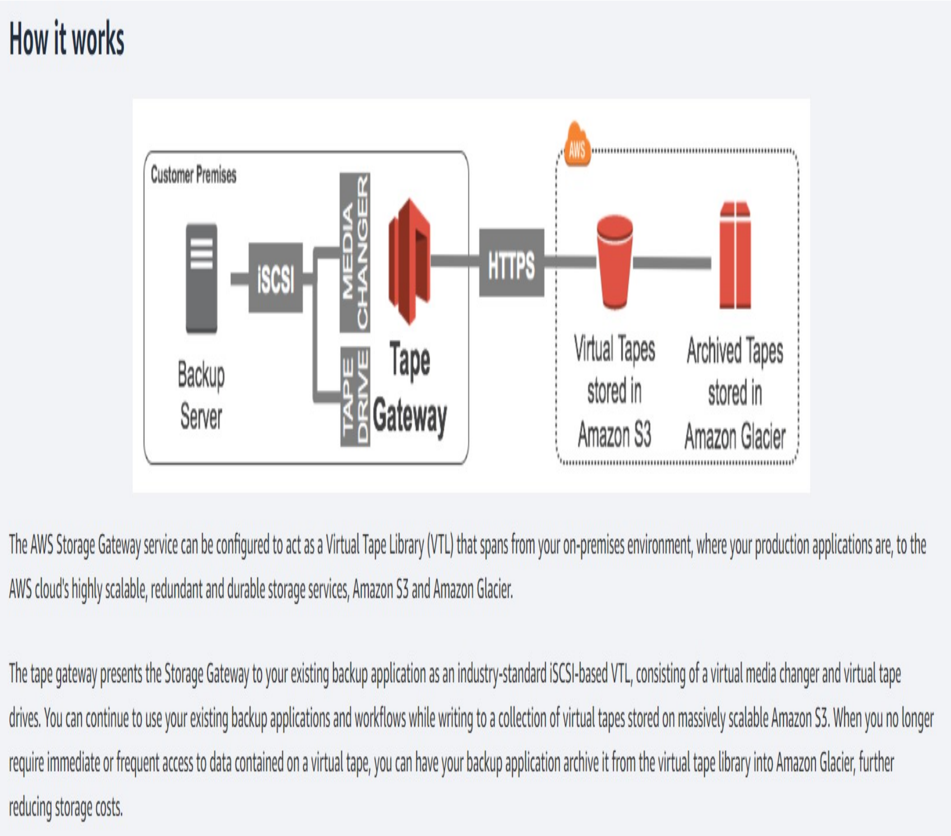
○ **B.** Make use of the AWS Storage gateway ✓

○ **C.** Store all the tape data on EBS volumes

○ **D.** Store all the tape data in Amazon Simple Storage Service

Explanation :

Answer – B
The AWS Documentation mentions the following



How it works

The AWS Storage Gateway service can be configured to act as a Virtual Tape Library (VTL) that spans from your on-premises environment, where your production applications are, to the AWS cloud's highly scalable, redundant and durable storage services, Amazon S3 and Amazon Glacier.

The tape gateway presents the Storage Gateway to your existing backup application as an industry-standard iSCSI-based VTL, consisting of a virtual media changer and virtual tape drives. You can continue to use your existing backup applications and workflows while writing to a collection of virtual tapes stored on massively scalable Amazon S3. When you no longer require immediate or frequent access to data contained on a virtual tape, you can have your backup application archive it from the virtual tape library into Amazon Glacier, further reducing storage costs.

Option A is invalid since even though Glacier is used for archive data, when storing tape data, it is better to use the AWS Storage gateway service

Option C is invalid since EBS volumes is used for local storage for EC2 Instances
Option D is invalid since S3 is used for data that is frequently accessed
For more information on the AWS Storage gateway, please refer to the below URL

- https://aws.amazon.com/storagegateway/vtl/ (https://aws.amazon.com/storagegateway/vtl/)

Ask our Experts

QUESTION 50 UNATTEMPTED

You have a fleet of EC2 Instances. They need to have a shared data store. The size of the items will vary from 1KB to 300 MB. The maximum size of the data store will be 3TB. The data needs to have a consistent read view. There are few changes to the data with reasonably no conflicts. Which of the following would be the ideal data store for the fleet of Instances?

○ **A.** Elastic File System ✔

○ **B.** Amazon S3

○ **C.** Amazon EBS Volumes

○ **D.** Amazon DynamoDB

Explanation :

Answer – A
The following is mentioned in the AWS Documentation when it comes to the features of EFS
Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance.
Amazon EFS provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently-accessible storage for up to thousands of Amazon EC2 instances.
Option B is invalid since this is used for object level storage that is available from the Internet
Option C is invalid since this is used for local block level storage for EC2 Instances
Option D is invalid since this is used for NoSQL database and ideally not suitable for such large item data sizes
For more information on the EFS file system, please refer to the below URL

- https://aws.amazon.com/efs/faq/ (https://aws.amazon.com/efs/faq/)

Ask our Experts

QUESTION 51 UNATTEMPTED

You are the SysOps administrator for a company. The company has an application that connects and makes use of an AWS RDS system. The RDS system is running into a lot of issues. It has been noticed that the same types of queries are causing a performance hit on the database. Which of the following services can be incorporated to reduce the performance issues? Choose 2 answers from the options given below

□ **A.** AWS Read Replica's ✓

□ **B.** AWS ElastiCache ✓

□ **C.** AWS RDS Multi-AZ

□ **D.** AWS RDS Automated Backups

Explanation :

Answer – A and B
The AWS Documentation mentions the following
Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.
Amazon ElastiCache offers fully managed Redis and Memcached (https://aws.amazon.com/memcached/). Seamlessly deploy, run, and scale popular open source compatible in-memory data stores. Build data-intensive apps or improve the performance of your existing apps by retrieving data from high throughput and low latency in-memory data stores.
Option C is incorrect since this is used for high availability of the database
Option D is incorrect since this is used for maintaining backups for the database
For more information on read replica's and ElastiCache, please refer to the below URL

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

Ask our Experts 👍 👎

QUESTION 52 UNATTEMPTED

You have an application that is connecting to an RDS instance. You need to ensure that the application will continue to run even if the database becomes unresponsive. There should be the least amount of downtime incurred when the primary database becomes unresponsive. Which of the following would you implement?

○ **A.** Create a read replica. Make the application connect to the Read Replica

○ **B.** Enable Multi-AZ for the database ✓

○ **C.** Use a Cloudfront distribution

○ **D.** AWS RDS Automated Backups

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable
Options A and D are partially correct , but for better switchover incase of a failure , you can make use the Multi-AZ feature
Option C is incorrect since this is used for content delivery to users across the world
For more information on Multi-AZ, please refer to the below URL

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

Ask our Experts

QUESTION 53 UNATTEMPTED

Your company has a set of Windows 2012 servers. There are restrictions on the amount of storage that can be used by these servers and AWS is being looked as an option for providing storage to these servers. The volumes for these servers need to have NTFS file permissions. Which of the following would you use for this purpose?

○ **A.** AWS Storage volume gateway ✓

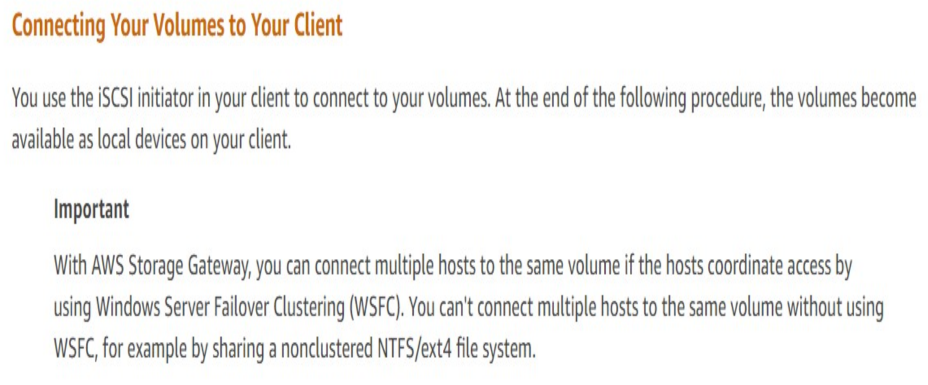
○ **B.** AWS Storage file gateway

○ **C.** AWS EFS

○ **D.** AWS S3

Explanation :

Answer – A
Options B and D are incorrect since the file gateway is used for object level storage
Option C is incorrect since this currently does not work for Windows based systems
You can use the Volume gateway to create volumes with NTFS file permissions



Connecting Your Volumes to Your Client

You use the iSCSI initiator in your client to connect to your volumes. At the end of the following procedure, the volumes become available as local devices on your client.

Important

With AWS Storage Gateway, you can connect multiple hosts to the same volume if the hosts coordinate access by using Windows Server Failover Clustering (WSFC). You can't connect multiple hosts to the same volume without using WSFC, for example by sharing a nonclustered NTFS/ext4 file system.

For more information on how to get started with using Volumes on the AWS Storage gateway, please refer to the below URL

- https://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStarted-use-volumes.html (https://docs.aws.amazon.com/storagegateway/latest/userguide/GettingStarted-use-volumes.html)

Ask our Experts

QUESTION 54 UNATTEMPTED

Your company has the following application in AWS which makes use of the following components

- A set of EC2 Instances serving a web application
- A Classic Load balancer set in front of the EC2 Instances
- An AWS RDS Instance

From the Cloudwatch metrics, you can see the high value for the "SpilloverCount". Which of the following should you monitor first to ensure that this metric does not increase in the first place?

○ **A.** SurgeQueueLength ✓

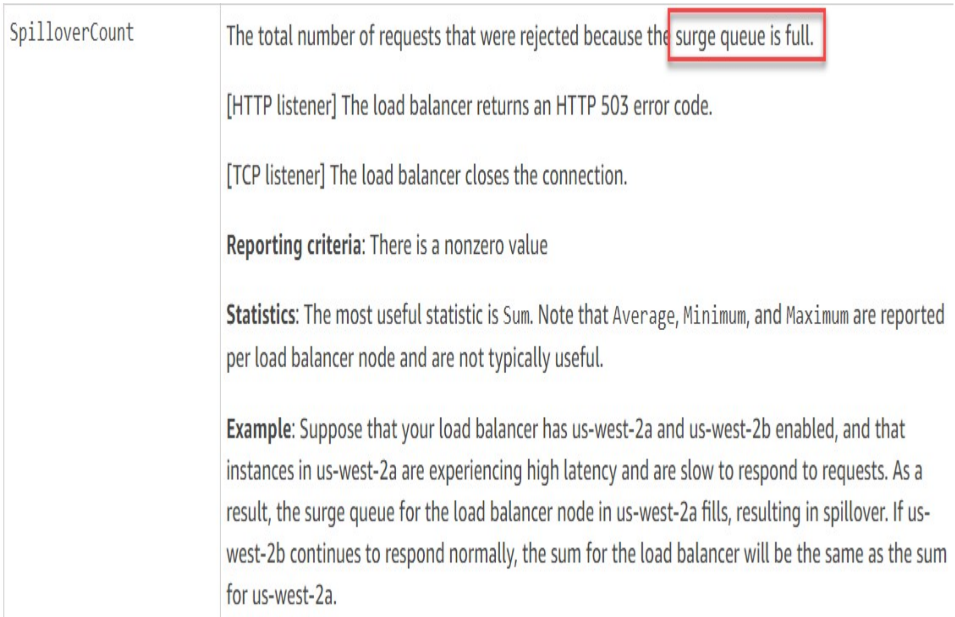
○ **B.** HealthyHostCount

○ **C.** BackendConnectionErrors

○ **D.** CPU Utilization

Explanation :

Answer – A
This is clearly given in the AWS Documentation



SpilloverCount	The total number of requests that were rejected because the surge queue is full. [HTTP listener] The load balancer returns an HTTP 503 error code. [TCP listener] The load balancer closes the connection. **Reporting criteria**: There is a nonzero value **Statistics**: The most useful statistic is Sum. Note that Average, Minimum, and Maximum are reported per load balancer node and are not typically useful. **Example**: Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer node in us-west-2a fills, resulting in spillover. If us-west-2b continues to respond normally, the sum for the load balancer will be the same as the sum for us-west-2a.

Because this is clearly mentioned in the documentation , all other options are invalid

For more information on metrics for the Classic Load balancer, please refer to the below URL

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

Ask our Experts

QUESTION 55 UNATTEMPTED

A company is hosting an application in AWS. The on-premise department needs to whitelist the application based on the IP/s. Which AWS component/feature is the company ideally using which is resulting in the whitelisting of the IP address?

○ **A.** AWS Network Load Balancer ✓

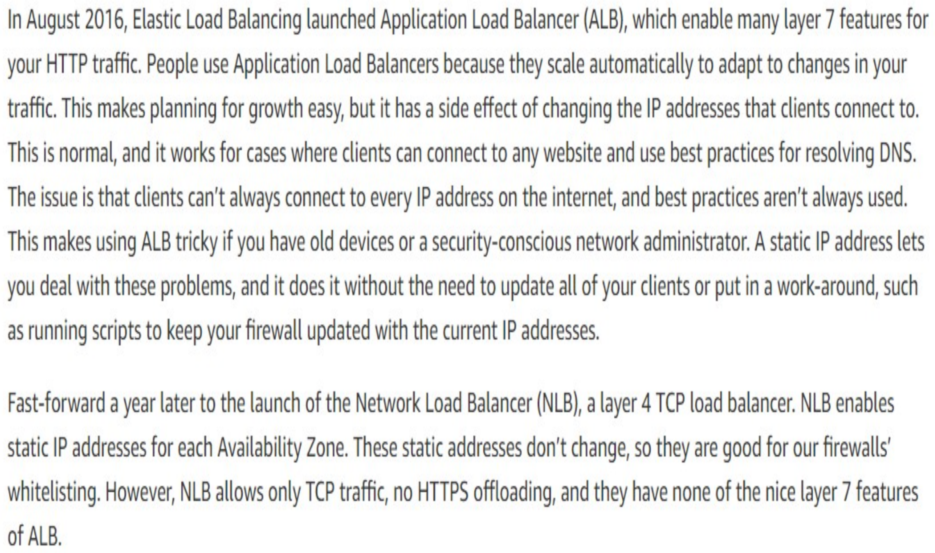
○ **B.** AWS Application Load Balancer

○ **C.** AWS Classic Load balancer

○ **D.** AWS Route 53

Explanation :

Answer – A
This is given in the AWS Documentation



In August 2016, Elastic Load Balancing launched Application Load Balancer (ALB), which enable many layer 7 features for your HTTP traffic. People use Application Load Balancers because they scale automatically to adapt to changes in your traffic. This makes planning for growth easy, but it has a side effect of changing the IP addresses that clients connect to. This is normal, and it works for cases where clients can connect to any website and use best practices for resolving DNS. The issue is that clients can't always connect to every IP address on the internet, and best practices aren't always used. This makes using ALB tricky if you have old devices or a security-conscious network administrator. A static IP address lets you deal with these problems, and it does it without the need to update all of your clients or put in a work-around, such as running scripts to keep your firewall updated with the current IP addresses.

Fast-forward a year later to the launch of the Network Load Balancer (NLB), a layer 4 TCP load balancer. NLB enables static IP addresses for each Availability Zone. These static addresses don't change, so they are good for our firewalls' whitelisting. However, NLB allows only TCP traffic, no HTTPS offloading, and they have none of the nice layer 7 features of ALB.

Options B and C are incorrect since you cannot allocate IP addresses to these Load balancers

Option D is incorrect since this is a domain name system
For more information on this use case scenario, please refer to the below URL

- https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/ (https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/)

Ask our Experts

QUESTION 56 UNATTEMPTED

Your company is working on creating a set of Cloudformation stacks. You need to create the stacks for the Operations department. You want to ensure that you are able to manually correct the errors? How can you achieve this?

○ **A.** Set the DeleteAPI for the stack to None

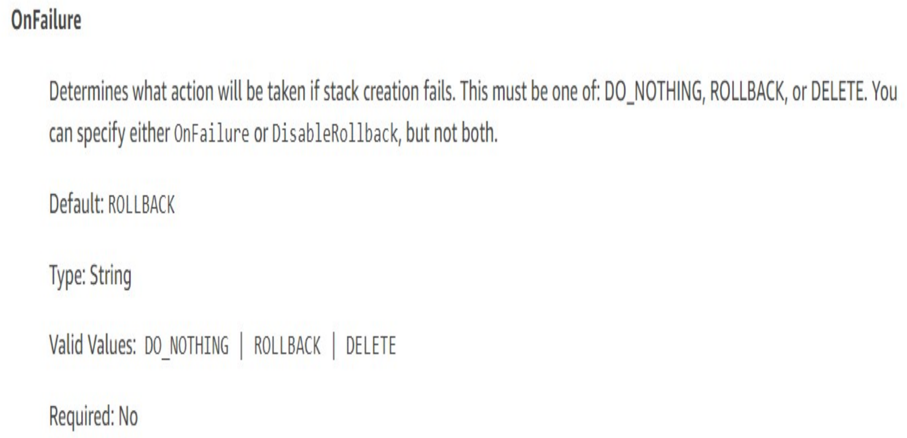
○ **B.** Set the OnFailure to DO_NOTHING when creating the stack ✔

○ **C.** Enable Termination protection on the stack

○ **D.** Set the ForceAPI for the stack as DO_NOT_DELETE

Explanation :

Answer - B
This is given in the AWS Documentation



OnFailure

Determines what action will be taken if stack creation fails. This must be one of: DO_NOTHING, ROLLBACK, or DELETE. You can specify either `OnFailure` or `DisableRollback`, but not both.

Default: `ROLLBACK`

Type: String

Valid Values: `DO_NOTHING | ROLLBACK | DELETE`

Required: No

Since this is clearly mentioned in the documentation, all other options are invalid

For more information on creating the stack via the API, please refer to the below URL

- https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html)

Ask our Experts

QUESTION 57 UNATTEMPTED

Your team is creating a number of Cloudformation stacks for multiple teams. There is request to ensure that the AWS RDS Instance which is created as part of the stack is retained for future purposes when the stack is deleted. How can you achieve this?

○ **A.** Set the DeleteAPI for the stack to None

○ **B.** Set the OnFailure to DO_NOTHING when creating the stack

○ **C.** Enable Termination protection on the stack

○ **D.** Use the DeletionPolicy attribute for the stack resource ✓

Explanation :

Answer - D
This is given in the AWS Documentation
With the DeletionPolicy attribute you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default.
Since this is clearly mentioned in the documentation, all other options are invalid
For more information on the deletion policy attribute, please refer to the below URL

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html)

Ask our Experts

QUESTION 58 UNATTEMPTED

You work as a SysOps Administrator for a company. The IT Management department want all systems hosted in AWS for their company to be up and running with few outrages also. You need to be notified in case any issues occur to the underlying hardware that hosts the AWS resources. Which of the following can help you achieve this?

○ **A.** Use the AWS Trusted Advisor tool

○ **B.** Use the Personal Health Dashboard ✓

○ **C.** Use the AWS Config tool

○ **D.** Use the AWS Cloudtrail tool

Explanation :

Answer – B
This is given in the AWS Documentation:
##############
AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources. The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.
################

- Option A is incorrect since this tool can only give you recommendations
- Option C is incorrect since this is only a config tool
- Option D is incorrect since is an API monitoring tool
- For more information on the personal health dashboard, please refer to the below URL
  - https://aws.amazon.com/premiumsupport/phd/ (https://aws.amazon.com/premiumsupport/phd/)

Ask our Experts

QUESTION 59 UNATTEMPTED

Your company is planning on hosting a set of databases using the AWS RDS service. The IT security department has mandated that all traffic is encrypted in transit. How can you achieve this with a database instance created with the AWS RDS service? Choose 2 answers from the options given below.

□ **A.** Use the SSL certificates provided by the AWS RDS service ✓

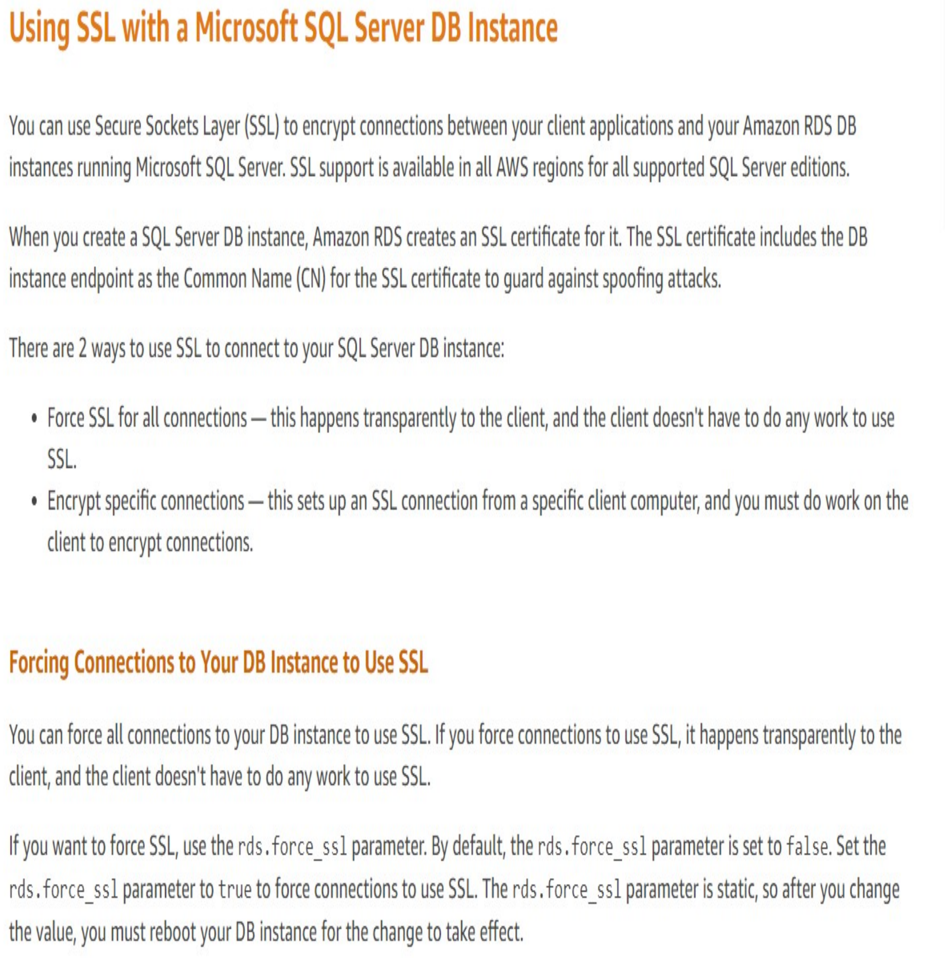
□ **B.** Set the Parameter Group for the RDS Instance ✓

□ **C.** Use the .pem keys files that come for the underlying server

□ **D.** Use the KMS service to encrypt the traffic

Explanation :

Answer – A and B
This is given in the AWS Documentation. An example for the Microsoft SQL server is given below



Using SSL with a Microsoft SQL Server DB Instance

You can use Secure Sockets Layer (SSL) to encrypt connections between your client applications and your Amazon RDS DB instances running Microsoft SQL Server. SSL support is available in all AWS regions for all supported SQL Server editions.

When you create a SQL Server DB instance, Amazon RDS creates an SSL certificate for it. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

There are 2 ways to use SSL to connect to your SQL Server DB instance:

- Force SSL for all connections — this happens transparently to the client, and the client doesn't have to do any work to use SSL.
- Encrypt specific connections — this sets up an SSL connection from a specific client computer, and you must do work on the client to encrypt connections.

Forcing Connections to Your DB Instance to Use SSL

You can force all connections to your DB instance to use SSL. If you force connections to use SSL, it happens transparently to the client, and the client doesn't have to do any work to use SSL.

If you want to force SSL, use the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to `false`. Set the `rds.force_ssl` parameter to `true` to force connections to use SSL. The `rds.force_ssl` parameter is static, so after you change the value, you must reboot your DB instance for the change to take effect.

Option C is incorrect since you don't have access to the underlying server

Option D is incorrect since the KMS service can't be used to encrypt the traffic
For more information on this example please refer to the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Concepts.General.SSL.Using.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Concepts.General.SSL.Using.html)

Ask our Experts

QUESTION 60 UNATTEMPTED

Your company has setup an architecture which consists of files hosted in an S3 bucket. And a Cloudfront distribution in front of the S3 bucket which is used to distribute content to the users. There are a certain number of 4xx errors which are coming as responses to the requests to Cloudfront. Which of the following can be possible reasons for such errors? Choose 2 answers from the options given below.

□ **A.** The user does not have access to the underlying bucket ✔

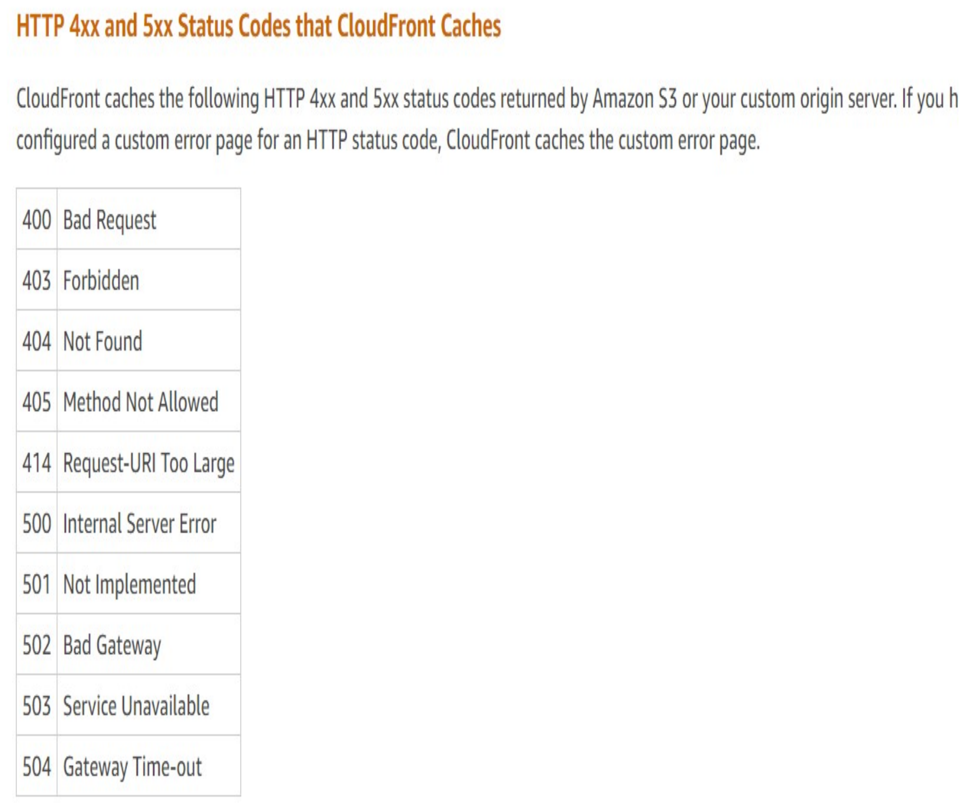
□ **B.** The Cloudfront service is unavailable

□ **C.** The object which the user is requesting for is not present ✔

□ **D.** There is an Internal server error

Explanation :

Answer – A and C
The AWS Documentation provides the different status codes.



HTTP 4xx and 5xx Status Codes that CloudFront Caches

CloudFront caches the following HTTP 4xx and 5xx status codes returned by Amazon S3 or your custom origin server. If you h configured a custom error page for an HTTP status code, CloudFront caches the custom error page.

400	Bad Request
403	Forbidden
404	Not Found
405	Method Not Allowed
414	Request-URI Too Large
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Time-out

Options B and D are incorrect since these pertain to 5xx errors

For more information on the HTTP Status error codes, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HTTPStatusCodes.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HTTPStatusCodes.html)

Ask our Experts 👍 👎

QUESTION 61 UNATTEMPTED

Your company is planning on setting up servers in a private subnet in a VPC. There is a requirement for the Instances in the private subnet to access an S3 bucket. You need to ensure that the traffic does not traverse the Internet. Which of the following is the ideal component to be used in this scenario?

○ **A.** NAT gateway

○ **B.** NAT Instance

○ **C.** VPC Endpoint ✓

○ **D.** Internet gateway

Explanation :

Answer – C
The AWS Documentation mentions the following
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.
All other options are invalid, since in these options the traffic would traverse the Internet
For more information on VPC Endpoints, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html)

Ask our Experts 👍 👎

QUESTION 62 UNATTEMPTED

You've just setup a custom VPC. You've launched Instances in a subnet in the custom VPC. You've noticed that the Instances are not receiving a public DNS hostname. Which of the following could be possible reasons for this? Choose 2 answers from the options given below.

□ **A.** enableDnsHostNames is set to No ✔

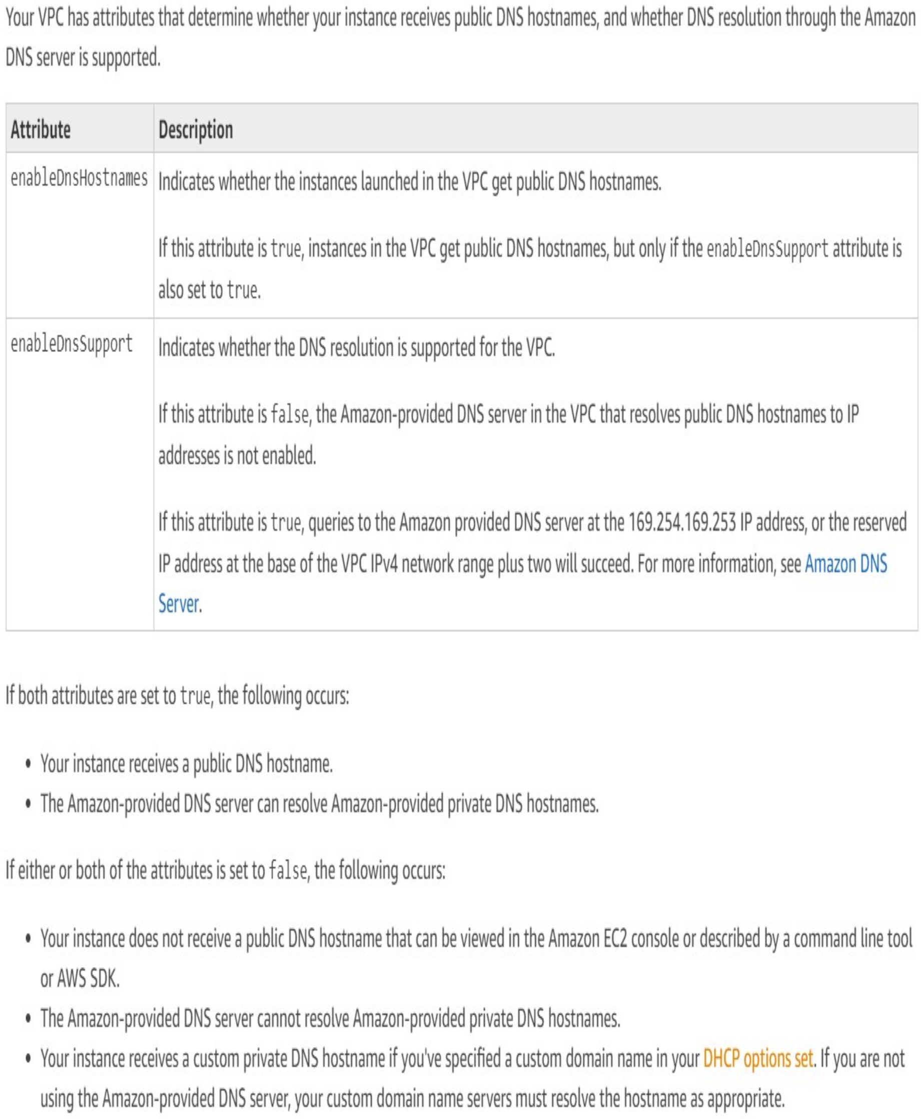
□ **B.** There is no Internet gateway attached to the VPC

□ **C.** The route tables have not been modified to include the Internet gateway

□ **D.** enableDnsSupport is set to No ✔

Explanation :

Answer A and D
The AWS Documentation mentions the following



Your VPC has attributes that determine whether your instance receives public DNS hostnames, and whether DNS resolution through the Amazon DNS server is supported.

Attribute	Description
`enableDnsHostnames`	Indicates whether the instances launched in the VPC get public DNS hostnames. If this attribute is `true`, instances in the VPC get public DNS hostnames, but only if the `enableDnsSupport` attribute is also set to `true`.
`enableDnsSupport`	Indicates whether the DNS resolution is supported for the VPC. If this attribute is `false`, the Amazon-provided DNS server in the VPC that resolves public DNS hostnames to IP addresses is not enabled. If this attribute is `true`, queries to the Amazon provided DNS server at the 169.254.169.253 IP address, or the reserved IP address at the base of the VPC IPv4 network range plus two will succeed. For more information, see Amazon DNS Server.

If both attributes are set to `true`, the following occurs:

- Your instance receives a public DNS hostname.
- The Amazon-provided DNS server can resolve Amazon-provided private DNS hostnames.

If either or both of the attributes is set to `false`, the following occurs:

- Your instance does not receive a public DNS hostname that can be viewed in the Amazon EC2 console or described by a command line tool or AWS SDK.
- The Amazon-provided DNS server cannot resolve Amazon-provided private DNS hostnames.
- Your instance receives a custom private DNS hostname if you've specified a custom domain name in your DHCP options set. If you are not using the Amazon-provided DNS server, your custom domain name servers must resolve the hostname as appropriate.

Since this is clearly mentioned in the documentation, all other options are invalid

For more information on VPC DNS, please refer to the below URL

- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html)

Ask our Experts 👍 👎

QUESTION 63 UNATTEMPTED

A development team needs to quickly deploy a container-based application onto AWS. They don’t want the headache of managing the application infrastructure. Which of the following service can be used to fulfil this requirement?

○ **A.** AWS Opswork

○ **B.** AWS Elastic Beanstalk ✓

○ **C.** AWS Cloudformation

○ **D.** AWS EC2

Explanation :

Answer – B
The AWS Documentation mentions the following
Elastic Beanstalk supports the deployment of web applications from Docker containers. With Docker containers, you can define your own runtime environment. You can choose your own platform, programming language, and any application dependencies (such as package managers or tools), that aren't supported by other platforms. Docker containers are self-contained and include all the configuration information and software your web application requires to run. All environment variables defined in the Elastic Beanstalk console are passed to the containers.
By using Docker with Elastic Beanstalk, you have an infrastructure that automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.
Option A is invalid since this environment should be used when you also want to use configuration management tool such as Chef and Puppet
Option C is invalid since this is used to deploy infrastructure as code
Option D is invalid since here the team would need to manage the infrastructure
For more information on Elastic Beanstalk, please refer to the below URL

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_docker.html)

Ask our Experts 👍 👎

QUESTION 64 UNATTEMPTED

A media company is currently making use of a number of AWS resources. One of them is a set of DynamoDB tables. They want to reduce the latency of the requests made to the DynamoDB table. Which of the following can help fulfil this requirement?

○ **A.** Use DAX ✓

○ **B.** Use Global tables

○ **C.** Use Secondary Indexes

○ **D.** Use DynamoDB streams

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache (https://aws.amazon.com/caching/) for DynamoDB (https://aws.amazon.com/dynamodb/) that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management.
Option B is invalid since this is used to create a multi-master database
Option C is invalid since this is used when you want to query data in the table via indexes
Option D is invalid since this is used when you want to be notified of changes in data to a DynamoDB table
For more information on DynamoDB DAX, please refer to the below URL

- https://aws.amazon.com/dynamodb/dax/ (https://aws.amazon.com/dynamodb/dax/)

Ask our Experts 👍 👎

QUESTION 65 UNATTEMPTED

You work as a SysOps Administrator for a company. The company has a large number of EC2 Instances and EBS volumes. There is a requirement for business continuity to ensure that the EBS volumes are available in another region in case the primary region fails. How can you achieve this?

○ **A.** Create a copy of the volume in another region.

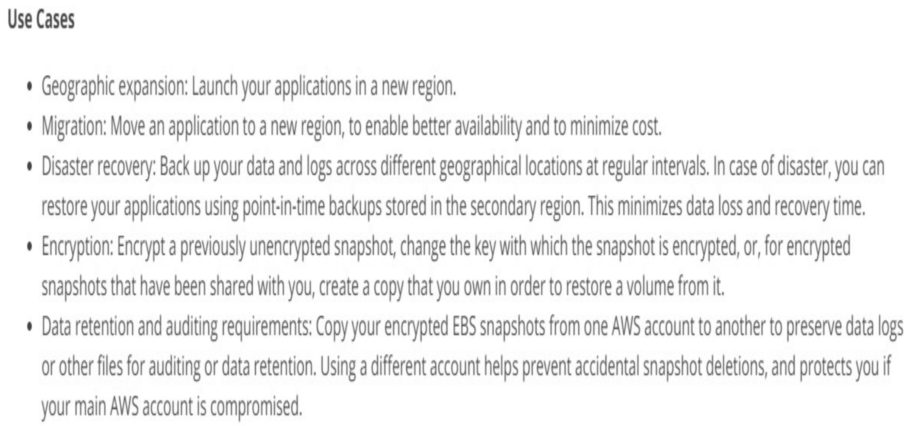
○ **B.** Create a snapshot from the volume in another region.

○ **C.** Create a snapshot. Copy the snapshot to the new region. ✓

○ **D.** Create a copy of the volume. Copy the volume to the new region.

Explanation :

Answer – C
The below snippet from the AWS Documentation showcases the use cases of EBS snapshots



Use Cases

- Geographic expansion: Launch your applications in a new region.
- Migration: Move an application to a new region, to enable better availability and to minimize cost.
- Disaster recovery: Back up your data and logs across different geographical locations at regular intervals. In case of disaster, you can restore your applications using point-in-time backups stored in the secondary region. This minimizes data loss and recovery time.
- Encryption: Encrypt a previously unencrypted snapshot, change the key with which the snapshot is encrypted, or, for encrypted snapshots that have been shared with you, create a copy that you own in order to restore a volume from it.
- Data retention and auditing requirements: Copy your encrypted EBS snapshots from one AWS account to another to preserve data logs or other files for auditing or data retention. Using a different account helps prevent accidental snapshot deletions, and protects you if your main AWS account is compromised.

Options A and D are incorrect , since you need to create a snapshot

Option B is incorrect since you cannot directly create a snapshot in another region
For more information on EBS Snapshot copy, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14843)

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/)

Company

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

- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

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

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

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

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