NEW PRACTICE TEST II

Attempt	1
Marks Obtained	1 / 65
Your score is	1.54%

Completed on	Tuesday , 29 January 2019 , 01:32 PM
Time Taken	00 H 00 M 15 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	64	1	0	63
2	Security and Compliance	1	0	0	1

65 Questions	**1** Correct	**0** Incorrect	**64** Unattempted

Show Answers

All

QUESTION 1 CORRECT

Your team has developed a set of Lambda functions. You have been asked to deploy these functions re-usable templates. These templates could then be subsequently deployed in other AWS environments. Which of the following service would you utilize to fulfil this requirement?

- A. AWS Opswork
- B. AWS Cloudformation ✔
- C. AWS Cloudtrail
- D. AWS Config

Explanation :

Answer – B
The AWS Documentation mentions the following
You can use AWS CloudFormation to specify, deploy, and configure serverless applications. AWS CloudFormation is a service that helps you model and set up your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all of the AWS resources that you want (like Lambda functions and DynamoDB tables), and AWS CloudFormation takes care of provisioning and configuring those resources for you. You don't need to individually create and configure AWS resources and figure out what's dependent on what—AWS CloudFormation handles all of that.
Option A is invalid since this is normally used along with configuration management tools such as Puppet and Chef
Option C is invalid since this is an API monitoring tool
Option D is invalid since this is a configuration service
For more information on deployment AWS Lambda via Cloudformation , please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/deploying-lambda-apps.html (https://docs.aws.amazon.com/lambda/latest/dg/deploying-lambda-apps.html)

Ask our Experts

QUESTION 2 UNATTEMPTED

You are the administrator for your company. You have setup Instances in a Custom VPC. You have set the Security groups and Network ACL's for the Instances and subnets respectively. The desired traffic is not reaching the instance. You need to diagnose the issue and see why the traffic is not reaching the instance. Which of the following would help in such a situation?

- A. Usage of AWS CloudWatch logs

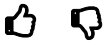
- B. Usage of AWS VPC Flow logs ✔
- C. Usage of AWS Cloudtrail logs
- D. Usage of AWS Trusted Advisor

Explanation :

Answer – B
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. Flow logs can help you with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance, which in turn helps you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.
Option A is invalid since this will not give you the detailed traffic logs
Option C is invalid since this is an API monitoring tool
Option D is invalid since this can only give you recommendations but not tell you why the traffic is being blocked
For more information on VPC Flow Logs, please refer to the below URL

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

Ask our Experts



QUESTION 3 UNATTEMPTED

You have a set of Instances defined in a private subnet in a VPC. These Instances need to download updates from the Internet. Below are the key requirements.

- Less maintenance in managing the device for relaying traffic
- Less restriction on bandwidth capabilities

Which of the following would you use for this requirement?

- A. NAT Instance
- B. Internet gateway
- C. NAT gateway ✔
- D. VPN Connection

Explanation :

Answer – C
When you look at the difference between the NAT Instance and the NAT gateway, you will see that the NAT gateway will meet the requirements

Comparison of NAT Instances and NAT Gateways

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.
Maintenance	Managed by AWS.You do not need to perform any maintenance.	Managed by you, for example, by installing software updates or operating system patches on the instance.
Performance	Software is optimized for handling NAT traffic.	A generic Amazon Linux AMI that's configured to perform NAT.
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Type and size	Uniform offering; you don't need to decide on the type or size.	Choose a suitable instance type and size, according to your predicted workload.
Public IP addresses	Choose the Elastic IP address to associate with a NAT gateway at creation.	Use an Elastic IP address or a public IP address with a NAT instance. You can change the public IP address at any time by associating a new Elastic IP address with the instance.

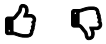
Option A is invalid since this would not fit the key requirements of less maintenance overhead and bandwidth capabilities

Option B is invalid since this would expose the private subnet and it would become a public subnet
Option D is invalid since this is used for hybrid connectivity

For more information on NAT gateways vs NAT Instances, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-comparison.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-comparison.html)

Ask our Experts



QUESTION 4 UNATTEMPTED

You have 2 VPC's , VPCA(10.0.0.0/16) and VPCB(20.0.0.0/16). You create a VPC peering connection which has an id of pcx-1a2b1a2b between the 2 VPC's. Which of the following route entries need to be added to the route tables to ensure that traffic can flow across the VPC's. Choose 2 answers from the options given below

- ☐ **A.** In VPCA (Destination:20.0.0.0/16 and Target: pcx-1a2b1a2b) ✔
- ☐ **B.** In VPCA (Destination:10.0.0.0/16 and Target: pcx-1a2b1a2b)
- ☐ **C.** In VPCA (Destination:20.0.0.0/16 and Target: 10.0.0.0/16)
- ☐ **D.** In VPCB (Destination:10.0.0.0/16 and Target: pcx-1a2b1a2b) ✔
- ☐ **E.** In VPCB (Destination:10.0.0.0/16 and Target: 20.0.0.0/16)

Explanation :

Answer – A and D
The AWS Documentation gives an example on this

For example, you have a VPC peering connection (pcx-1a2b1a2b) between two VPCs, with the following information:

- VPC A: vpc-1111aaaa, CIDR block is 10.0.0.0/16
- VPC B: vpc-2222bbbb, CIDR block is 172.31.0.0/16

To enable traffic between the VPCs and allow access to the entire IPv4 CIDR block of either VPC, the VPC A route table is configured as follows.

Destination	Target
10.0.0.0/16	Local
172.31.0.0/16	pcx-1a2b1a2b

The VPC B route table is configured as follows.

Destination	Target
172.31.0.0/16	Local
10.0.0.0/16	pcx-1a2b1a2b

Because of what is given in the documentation , the other options are invalid

For more information on this example, please refer to the below URL

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

Ask our Experts

QUESTION 5 UNATTEMPTED

You work as a Systems Administrator for a company. You have created an AWS RDS-MySQL Instance. Manual snapshots of the database are carried out from time to time for disaster recover drill scenarios. The company has a requirement to ensure there is no downtime when a snapshot is created for the database. How can you ensure this?

- A. Ensure that the snapshot is only taken during the maintenance window
- B. Ensure that Multi-AZ is enabled for the database ✔

- C. Ensure that the underlying volume type for the database is IOPS
- D. Ensure that the underlying volume type for the database is SSD

Explanation :

Answer – B
The AWS Documentation mentions the following
Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Creating this DB snapshot on a Single-AZ DB instance results in a brief I/O suspension that can last from a few seconds to a few minutes, depending on the size and class of your DB instance. Multi-AZ DB instances are not affected by this I/O suspension since the backup is taken on the standby.
Option A is incorrect because this would still result in an outage
Options C and D are incorrect since the underlying volumes have no impact on the outage
For more information on creating snapshots, please refer to the below URL

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

Ask our Experts

QUESTION 6 UNATTEMPTED

You are the Systems Administrator for a company. There is a requirement for a consultant to view the contents of an S3 bucket in the company's AWS account. The time required for the access is limited. Which of the following would be used to control the access?

- A. Create an IAM user with a session duration parameter
- B. Create an IAM Role with a session duration parameter ✔
- C. Specify a time limit in the Bucket ACL.
- D. Grants access keys based on a time interval

Explanation :

Answer – B
The AWS Documentation mentions the following
When you use an AWS CLI or API operation to assume a role, you can specify a value for the DurationSeconds parameter. You can use this parameter to specify the duration of the role session, from 900 seconds (15 minutes) up to the Maximum CLI/API session duration setting for the role. Before you specify the parameter, you should view this setting for your role. If you specify a value for the DurationSeconds parameter that is higher than the maximum setting, the operation fails.
All other options are invalid because such options cannot be implemented
For more information on setting the IAM Role duration, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html#id_roles_use_view-role-max-session
(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html#id_roles_use_view-role-max-session)

Ask our Experts

QUESTION 7 UNATTEMPTED

Your company is planning on hosting a static website in S3. The static website will be brought up when users browse to http://companya.com (http://companyA.com) domain. You have to create the bucket in S3. Which of the following should be the name assigned to the bucket?

- A. https://companyA.com
- B. companyA
- C. companya.com ✔
- D. s3. companyA.com

Explanation :

Answer – C
The AWS Documentation clearly mentions this.

The bucket names must match the names of the website that you are hosting. For example, to host your example.com website on Amazon S3, you would create a bucket named example.com. To host a website under www.example.com, you would name the bucket www.example.com. In this example, your website supports requests from both example.com and www.example.com.
Because of what the AWS Documentation mentions, all other options are invalid
For more information on setting an S3 bucket with a custom domain, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html)

Ask our Experts

QUESTION 8 UNATTEMPTED

A company has a bucket which has a set of documents. These documents have sensitive information. The IT Management staff need to be notified whenever a change is made to the documents in the S3 bucket. How can you achieve this? Choose 2 answers from the options given below

- ☐ **A.** Enable S3 server access logging
- ☐ **B.** Set up an S3 event notification ✔
- ☐ **C.** Create an SNS topic ✔
- ☐ **D.** Create an SQS queue

Explanation :

Answer – B and C
The AWS Documentation mentions the following

Amazon S3 can send notifications for the following events:

- **An object created event** - You choose **ObjectCreated (All)** when configuring your events in the console to enable notifications for anytime an object is created in your bucket. Or, you can select one or more of the specific object-creation actions to trigger event notifications. These actions are **Put**, **Post**, **Copy**, and **CompleteMultiPartUpload**.
- **An object delete event** - You select **ObjectDelete (All)** when configuring your events in the console to enable notification for anytime an object is deleted. Or, you can select **Delete** to trigger event notifications when an unversioned object is deleted or a versioned object is permanently deleted. You select **Delete Marker Created** to trigger event notifications when a delete marker is created for a versioned object.
- **A Reduced Redundancy Storage (RRS) object lost event** - You select **RRSObjectLost** to be notified when Amazon S3 detects that an object of the RRS storage class has been lost.

Event notification messages can be sent to the following types of destinations:

- **An Amazon Simple Notification Service (Amazon SNS) topic** - A web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.
- **An Amazon Simple Queue Service (Amazon SQS) queue** - Offers reliable and scalable hosted queues for storing messages as they travel between computer.
- **A Lambda function** - AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure. You package up and upload your custom code to AWS Lambda when you create a Lambda function

Option A is invalid because you need to use S3 event notification.

Option D is invalid because you need to use for email notifications
For more information on event notifications, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-event-notifications.html (https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-event-notifications.html)

Ask our Experts

QUESTION 9 UNATTEMPTED

A company has a set of Hadoop clusters running on their On-premise environment. They want to transfer them to AWS. Which of the following would be the ideal service you would use to transition the existing workload?

- A. AWS Redshift
- B. AWS DynamoDB

- C. AWS EMR ✔
- D. AWS RDS

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon EMR is a managed cluster platform that simplifies running big data frameworks, such as Apache Hadoop (https://aws.amazon.com/elasticmapreduce/details/hadoop) and Apache Spark (https://aws.amazon.com/elasticmapreduce/details/spark), on AWS to process and analyze vast amounts of data. By using these frameworks and related open-source projects, such as Apache Hive and Apache Pig, you can process data for analytics purposes and business intelligence workloads. Additionally, you can use Amazon EMR to transform and move large amounts of data into and out of other AWS data stores and databases, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB.
Option A is incorrect since this is used for data warehousing solutions
Option B is incorrect since this is used for NoSQL databases
Option D is incorrect since is used for hosting relational databases
For more information on AWS EMR, please refer to the below URL

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

Ask our Experts

QUESTION 10 UNATTEMPTED

Your company is planning on creating an AWS RDS Instance. The IT Security department has stated that all data must be encrypted at rest. Which of the following is the easiest way to achieve this?

- A. Encrypt all the data that gets stored in the database
- B. Encrypt the underlying database volumes
- C. Enable encryption when the database is being created ✔
- D. Apply encryption to an existing database

Explanation :

Answer – C
Options A and B are not proper operations that can be implemented
Option D is invalid you can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created
The AWS Documentation mentions the following
You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance. Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots.
Amazon RDS encrypted instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS instance. Once your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. You don't need to modify your database client applications to use encryption.
For more information on AWS RDS Encryption, please refer to the below URL

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

Ask our Experts

QUESTION 11 UNATTEMPTED

A company is hosting a social media application on AWS. The application makes use of DynamoDB as the backend. The read and write capacity has already been defined for the table. But it has been noticed that during high peak loads, the database begins throttling requests. Which of the following can be used to effectively manage the high number of requests during high peak loads?

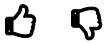
- A. Place an ELB in front of the DynamoDB table
- B. Add the DynamoDB table to an Autoscaling Group
- C. Enable Autoscaling for the DynamoDB table ✔
- D. Place an SQS queue in front of the DynamoDB table

Explanation :

Answer - C
The AWS Documentation mentions the following
DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.
All other options are invalid since these are not the right principles to be followed when designing for high throughput on the DynamoDB table.
For more information on AWS DynamoDB Autoscaling, please refer to the below URL

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

Ask our Experts



QUESTION 12 UNATTEMPTED

You've just restored a volume from a snapshot and attached it to an EC2 Instance. This Instance hosts an application that is going to make use of the new EBS volume. You noticed some initial I/O latency when the application was first launched. How can you ensure that subsequent volumes created from the same snapshot don't face the similar issue?

- A. Ensure that the volume being created is of the volume type Provisioned IOPS
- B. Ensure that the volume being created is of the volume type General Purpose SSD
- C. Ensure that the volume is created in the same availability zone as the snapshot
- D. Ensure that all blocks on the volume are accessed at least once ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
New EBS volumes receive their maximum performance the moment that they are available and do not require initialization (formerly known as pre-warming). However, storage blocks on volumes that were restored from snapshots must be initialized (pulled down from Amazon S3 and written to the volume)

before you can access the block. This preliminary action takes time and can cause a significant increase in the latency of an I/O operation the first time each block is accessed. For most applications, amortizing this cost over the lifetime of the volume is acceptable. Performance is restored after the data is accessed once.
You can avoid this performance hit in a production environment by reading from all of the blocks on your volume before you use it; this process is called *initialization*. For a new volume created from a snapshot, you should read all the blocks that have data before using the volume.
Options A and B are incorrect because this does not depend on the underlying volume type
Option C is invalid since they need to anyway be in the same availability zone
For more information on initializing volumes, please refer to the below URL
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-initialize.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-initialize.html)

Ask our Experts

QUESTION 13 UNATTEMPTED

A company has a set of EC2 Instances hosted in a VPC. There is a requirement to perform a scan to see if there are any security vulnerabilities. The check needs to be done as per the Industry standards of the "Center for Internet Security (CIS) Benchmarks (https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html)". Which of the following can help you achieve this requirement?

- **A.** Use the AWS Trusted Advisor
- **B.** Use the AWS Inspector service ✔
- **C.** Use the AWS Config service
- **D.** Use the AWS GuardDuty service

Explanation :

Answer – B
The following are the rules packages available in Amazon Inspector:
· Common Vulnerabilities and Exposures

(https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cves.html)
· Center for Internet Security (CIS) Benchmarks
(https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html)
· Security Best Practices
(https://docs.aws.amazon.com/inspector/latest/userguide/inspector_security-best-practices.html)
· Runtime Behavior Analysis
(https://docs.aws.amazon.com/inspector/latest/userguide/inspector_runtime-behavior-analysis.html)

Hence you can use the AWS Inspector service to scan the Instances for vulnerabilities based on this package.
Option A is invalid since this can only give you various recommendations
Option C is invalid since this is a configuration service
Option D is invalid since this is a managed threat detection service
For more information on AWS Inspector, please refer to the below URL
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html
(https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html)

Ask our Experts

QUESTION 14 UNATTEMPTED

You have a set of EC2 Instances defined in AWS. To conserve on costs, you would like to shutdown the instances when the Instance is not being used. How can you accomplish this?

- **A.** Create cloudwatch alarms based on a certain metric and then shutdown the instance based on the alarm. ✔
- **B.** Check the cloudtrail logs to see if there is any activity on the instance. If not, then trigger an alert to shut down the instance
- **C.** Check the AWS Config service to check for any configuration changes on the instance. If there are no changes, then trigger an alert to shut down the instance
- **D.** Check the cloudwatch metrics on the underlying EBS volumes. If there is no activity , then you should trigger an alarm to shut down the instance

Explanation :

Answer – A
The AWS Documentation mentions the following
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 B is invalid because this will give you the API activity only
Option C is invalid because this will give you the configuration changes
Option D is invalid because the question does not mention how to check for the inactivity of the instance
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 15 UNATTEMPTED

Your company has created a set of resources in AWS. They want to ensure that they do not exceed the limit on certain services beforehand. Which of the following can help in this regard?

- A. AWS Config
- B. AWS Trusted Advisor ✔
- C. AWS Personal Health Dashboard
- D. AWS Inspector

Explanation :

Answer – B
The AWS Documentation mentions the following

AWS Trusted Advisor (https://aws.amazon.com/premiumsupport/trustedadvisor/) offers a Service Limits check (in the Performance category) that displays your usage and limits for some aspects of some services
Option A is invalid because this is a configuration service
Option C is invalid because this will give you the health of the underlying AWS hardware
Option D is invalid because this is used to conduct vulnerability assessments
For more information on the service limits, please refer to the below URL

- https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html (https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html)

Ask our Experts

QUESTION 16 UNATTEMPTED

Your development team has set an application on an EC2 Instance. This instance is currently sitting in a private subnet. The application needs to make use of Kinesis streams. How would you ensure that the application would be able to make use of the Kinesis streams service?

- A. Ensure that an Internet gateway is attached to the VPC
- B. Ensure that an Egress-only Internet gateway
- C. Use a VPC Endpoint gateway
- D. Use a VPC Endpoint Interface ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC.
Option A is incorrect since the Instance should not be moved to a public subnet just for this type of access
Option B is incorrect since this is used for IPv6 traffic specifically

Option C is incorrect since this is only used with the S3 and DynamoDB service
For more information on using streams within a VPC, please refer to the below URL

- https://docs.aws.amazon.com/streams/latest/dev/vpc.html
(https://docs.aws.amazon.com/streams/latest/dev/vpc.html)

Ask our Experts

QUESTION 17 UNATTEMPTED

Your company is planning on hosting a web application on a set of EC2 Instances. Based on the initial response, it has now been decided to add service which would help distribute the traffic across a set of EC2 Instances hosting the application. The main requirements are that the service should be able to scale to a million requests. Which of the following would you implement for this requirement?

- **A.** An ECS Cluster
- **B.** A Network Load balancer ✔
- **C.** A Classic Load Balancer
- **D.** An SQS queue

Explanation :

Answer – B
The AWS Documentation mentions the following
Using a Network Load Balancer instead of a Classic Load Balancer has the following benefits:
· Ability to handle volatile workloads and scale to millions of requests per second.
· Support for static IP addresses for the load balancer. You can also assign one Elastic IP address per subnet enabled for the load balancer.
· Support for registering targets by IP address, including targets outside the VPC for the load balancer.

Option A is incorrect since there is no specific mention in the question on Docker containers
Option C is incorrect since you need a network load balancer for higher throughput of requests
Option D is incorrect since there is no mention on the need for distribution of messages between components of the application.

For more information on the network load balancer, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html)

Ask our Experts

QUESTION 18 UNATTEMPTED

A team has developed an application that works with a DynamoDB table. This application is now going to be hosted on an EC2 Instance. Which of the following would you do from an implementation purpose to ensure that the application has the relevant permissions to access the DynamoDB table?

- **A.** Create an IAM user with the required permissions and ensure the application runs on behalf of the user on the EC2 instance
- **B.** Create an IAM group with the required permissions and ensure the application runs on behalf of the group on the EC2 instance
- **C.** Create an IAM Role with the required permissions and ensure that the Role is assigned to the EC2 Instance ✔
- **D.** Create Access keys with the required permissions and ensure that the Access keys are embedded in the application

Explanation :

Answer – C
This is also given in the AWS documentation

When to Create an IAM Role (Instead of a User)

Create an IAM role in the following situations:

You're creating an application that runs on an Amazon Elastic Compute Cloud (Amazon EC2) instance and that application makes requests to AWS.

Don't create an IAM user and pass the user's credentials to the application or embed the credentials in the application. Instead, create an IAM role that you attach to the EC2 instance to give applications running on the instance temporary security credentials. The credentials have the permissions specified in the policies attached to the role. For details, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances.

Options A and B are incorrect since you need to use IAM Roles

Option D is incorrect because embedding Access keys is not a secure way to access AWS resources from EC2 Instances
For more information on managing ID's in IAM, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html)

Ask our Experts

QUESTION 19 UNATTEMPTED

You work as a Systems Administrator for a company. The company has a number of resources hosted in AWS. An external audit is going to be conducted on the AWS resources. As part of the audit, you are required to give log files for all activity carried out on the existing AWS resources. Which of the following service would be able to fulfil this requirement?

- A. AWS Cloudwatch logs
- B. AWS Trusted Advisor
- C. AWS Config
- D. AWS Cloudtrail ✔

Explanation :

Answer -D
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 invalid because this service will not give you all the Activity recorded for each AWS resource
Option B is invalid because since this can only give you recommendations
Option C is invalid because this is a configuration service
For more information on AWS 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 20 UNATTEMPTED

A company currently uses the Chef tool to manage the configuration on its underlying servers. They want to start provisioning servers on the AWS Cloud. They want to ensure that they can re-use their existing Chef recipes for configuration management. Which of the following service would be recommended to use in this regard?

- **A.** AWS ElasticBeanstalk
- **B.** AWS Cloudformation
- **C.** AWS EC2
- **D.** AWS Opswork ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
AWS OpsWorks is a configuration management service that helps you configure and operate applications in a cloud enterprise by using Puppet or Chef. AWS OpsWorks Stacks and AWS OpsWorks for Chef Automate let you use Chef (https://www.chef.io/) cookbooks and solutions for configuration management, while OpsWorks for Puppet Enterprise lets you configure a Puppet Enterprise (https://puppet.com/products/puppet-enterprise) master server in AWS. Puppet offers a set of tools for enforcing the desired state of your infrastructure, and automating on-demand tasks
Option A is invalid because this service is good for quickly provisioning environments but does not have out of the box support for the Chef tool
Option B is invalid because this service is used for developing templates which represent Infrastructure as code
Option C is invalid because this is the underlying compute service
For more information on AWS Opswork, please refer to the below URL

- https://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html (https://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html)

Ask our Experts

QUESTION 21 UNATTEMPTED

Your company has a set of Instances in a subnet in a VPC. These set of Instances host a web-based application. There are a number of similar types of requests coming from an IP address of 52.67.89.10. Your IT Security department has requested that all subsequent traffic from this IP address is blocked. How can you achieve this?

- **A.** Create an Outbound rule for the Security Group for the EC2 Instances to ensure that no traffic goes to that IP
- **B.** Create an Inbound Rule for the NACL which will deny traffic coming from 52.67.89.10/0
- **C.** Create an Inbound Rule for the NACL which will deny traffic coming from 52.67.89.10/32 ✔
- **D.** Create an Outbound Rule for the NACL which will deny traffic coming from 52.67.89.10/32

Explanation :

Answer – C
Since the request is an Inbound request from an IP, it must be stopped at the subnet level. So here you will add a rule to the Network Access control list
Option A is invalid because the rule needs to be added at the subnet level
Option B is invalid because this is an invalid CIDR range.
Option D is invalid because it should be a rule for Inbound traffic.
For more information on Network ACL's, please refer to the below URL

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

Ask our Experts

QUESTION 22 UNATTEMPTED

Your company is planning on hosting services in AWS and also planning on purchasing a support plan. Below are the key requirements

- 24x7 access to customer service
- Business hours access to Cloud Support Associates

Which of the following support plan would you choose ensuring that COST is kept to a minimum

- A. Basic
- B. Developer ✔
- C. Business
- D. Enterprise

Explanation :

Answer - B
This is given in the AWS Documentation

	Basic	Developer	Business	Enterprise
Customer Service and Communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best Practices	Access to 7 core Trusted Advisor checks	Access to 7 core Trusted Advisor checks	Access to full set of Trusted Advisor checks	Access to full set of Trusted Advisor checks
Health status and Notifications	Access to Personal Health Dashboard	Access to Personal Health Dashboard	Access to Personal Health Dashboard & Health API	Access to Personal Health Dashboard & Health API
Technical Support		Business hours** access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat & phone	24x7 access to Sr. Cloud Support Engineers via email, chat & phone

Based on what given in the AWS Documentation , you would choose the Developer Support plan

For more information on AWS Support plans, please refer to the below URL

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

Ask our Experts

QUESTION 23 UNATTEMPTED

Your company has a set of Linux based EC2 Instances. You need to generate reports on the memory usage for these set of Instances. These dashboards need to be viewed by the Linux Administrators team on a continuous basis. Which of the following steps would you need to implement for this requirement. Choose 2 answers from the options given below

- [ ] **A.** Ensure that the EC2 Instance Config tool is installed on the Linux instance
- [ ] **B.** Ensure that the Cloudwatch monitoring scripts are installed on the Linux Instances ✔
- [ ] **C.** Use Cloudtrail logs for logging all the metrics
- [ ] **D.** Use Cloudwatch for logging all the metrics ✔

Explanation :

Answer – B and D
The AWS Documentation mentions the following
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 invalid because this is used for Windows based instances
Option C is invalid because this is used for API monitoring
For more information on using monitoring scripts for your Linux based instances, 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 24 UNATTEMPTED

Your company has a set of EC2 Instances in AWS. Senior management wants to know the usage costs for the current set of EC2 Instances and also get a clear forecast in the future usage and costs. How can you go about fulfilling this requirement?

- A. By using the AWS Trusted Advisor
- B. By using the EC2 Explorer
- C. By using the Cost Explorer ✔
- D. By using the AWS Config tool

Explanation :

Answer – C
The AWS Documentation mentions the following
AWS provides a free reporting tool called Cost Explorer that enables you to analyze the cost and usage of your EC2 instances and the usage of your Reserved Instances.
Cost Explorer is a free tool that you can use to view charts of your usage and costs. You can view data up to the last 13 months and forecast how much you are likely to spend for the next three months. You can use Cost Explorer to see patterns in how much you spend on AWS resources over time, identify areas that need further inquiry, and see trends that you can use to understand your costs. You also can specify time ranges for the data, and view time data by day or by month.
Option A is invalid because this is a recommendations-based tool in AWS
Option B is invalid because this will give the listing of the EC2 resources but now the costs associated
Option D is invalid because this is a configuration-based tool
For more information on usage reports, please refer to the below URL

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

Ask our Experts

QUESTION 25 UNATTEMPTED

You've launched an EC2 Instance in a private subnet in a VPC. After the launch, you are seeing that an Instance status check has failed. Which of the following is a way you can try and resolve this issue?

- A. Make sure that the instance is launched in a public subnet instead of a private subnet
- B. Try rebooting the instance ✔

- **C.** Try changing the Security groups to allow the underlying hardware to make the necessary instance status checks
- **D.** Try changing the NACL's to allow the underlying hardware to make the necessary instance status checks

Explanation :

Answer – B
The AWS Documentation mentions the following
Instance Status Checks - monitor the software and network configuration of your individual instance. These checks detect problems that require your involvement to repair. When an instance status check fails, typically you will need to address the problem yourself (for example by rebooting the instance or by making modifications in your operating system). Examples of problems that may cause instance status checks to fail include:

- Failed system status checks
- Misconfigured networking or startup configuration
- Exhausted memory
- Corrupted file system
- Incompatible kernel

Option A is incorrect because this does not depend on which subnet the Instance is launched in.
Options C and D are incorrect since the security groups and NACL's don't have an effect on the status checks
For more information on monitoring your EC2 Instances, please refer to the below URL

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

Ask our Experts

QUESTION 26 UNATTEMPTED

You're planning on launching your first EC2 Instance on the AWS Cloud. This would be a Linux based instance which would be launched in the default VPC. Which of the following is the 2-part process which is followed which would be used subsequently for logging into the Instance. Choose 2 answers from the options given below

- [ ] **A.** The public key needs to be created and placed on the EC2 Instance ✔
- [ ] **B.** The private key needs to be created and placed on the EC2 Instance
- [ ] **C.** The public key needs to be used to log into the Instance
- [ ] **D.** The private key needs to be used to log into the Instance ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following
To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. On a Linux instance, the public key content is placed in an entry within ~/.ssh/authorized_keys. This is done at boot time and enables you to securely access your instance using the private key instead of a password.
Option B is incorrect since it is the public key that needs to be placed on the EC2 Instance
Option C is incorrect since the private key needs to be used to log into the Instance
For more information on EC2 Key pairs, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

A company currently has started using the Storage gateway service to extend its storage capacity to the AWS Cloud. There is a mandate that all data is encrypted when it is being managed by the AWS Storage gateway. Which of the following would you implement to comply with this request?

- ○ **A.** Create an X.509 certificate that can be used to encrypt the data
- ○ **B.** Use AWS KMS service to support encryption of the data. ✔
- ○ **C.** Use an SSL certificate to encrypt the data
- ○ **D.** Use your own master keys to encrypt the data

Explanation :

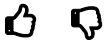
Answer - B
The AWS Documentation mentions the following
##############
AWS Storage Gateway uses AWS Key Management Service (AWS KMS) to support encryption. Storage Gateway is integrated with AWS KMS so you can use the customer master keys (CMKs) in your account to protect the data that Storage Gateway receives, stores, or manages. Currently, you can do this by using the AWS Storage Gateway API.
##############

- All other options are invalid since the right way to encrypt the data is via using KMS keys
- For more information on storage gateway encryption, please refer to the below URL
  - https://docs.aws.amazon.com/storagegateway/latest/userguide/encryption.html (https://docs.aws.amazon.com/storagegateway/latest/userguide/encryption.html)
  - As per AWS docs, Storage Gateway supports AWS KMS for encryption of data stored in AWS by all gateway types. This includes virtual tapes managed by Tape Gateway, in-cloud volumes and EBS Snapshots created by Volume Gateway, and files stored as objects in Amazon Simple Storage Service (S3) by File Gateway.

If AWS KMS is not used, all data stored in AWS by the Storage Gateway service is encrypted with Amazon S3-Managed Encryption Keys (SSE-S3) by default.

- Hence option B is the right choice.

Ask our Experts



QUESTION 28 UNATTEMPTED

A company currently uses a Redshift cluster for managing their data warehouse. There is a requirement now to ensure that all the data that gets transferred to the Redshift cluster is done via a VPC. As the Systems administrator, how would you accomplish this requirement?

- A. Change the Security Groups for the Cluster to only allow traffic into the VPC
- B. Enable Amazon Redshift Enhanced VPC Routing ✔
- C. Ensure that the underlying EBS volumes for the cluster are created in the VPC

D. Ensure that the settings are defined in the parameter group

Explanation :

Answer – B
The AWS Documentation mentions the following
When you use Amazon Redshift Enhanced VPC Routing, Amazon Redshift forces all COPY (http://docs.aws.amazon.com/redshift/latest/dg/r_COPY.html) and UNLOAD (http://docs.aws.amazon.com/redshift/latest/dg/r_UNLOAD.html) traffic between your cluster and your data repositories through your Amazon VPC. You can now use standard VPC features, such as VPC security groups (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html), network access control lists (ACLs) (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html), VPC endpoints (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints-s3.html), VPC endpoint policies (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints-s3.html#vpc-endpoints-policies-s3), Internet gateways (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html), and Domain Name System (DNS) (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html) servers, to tightly manage the flow of data between your Amazon Redshift cluster and other resources. When you use Enhanced VPC Routing to route traffic through your VPC, you can also use VPC flow logs (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html) to monitor COPY and UNLOAD traffic.
Options A and C are invalid since using either Security groups or modifying the EBS volumes will guarantee that the traffic moves via the VPC
Option D is invalid because parameter groups is a group of parameters that apply to all of the databases that you create in the cluster. These parameters configure database settings such as query timeout and date style
For more information on Enhanced VPC Routing, please refer to the below URL

- https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html (https://docs.aws.amazon.com/redshift/latest/mgmt/enhanced-vpc-routing.html)

Ask our Experts

QUESTION 29 UNATTEMPTED

Your company's development team currently have an application deployed on their on-premise environment. This application makes use of Docker containers. This application environment needs to be ported onto AWS. The development team does not want to manage the underlying infrastructure. Which of the following is the ideal service you would use to provision the environment for them?

- **A.** AWS ElasticBeanstalk ✔
- **B.** AWS EC2
- **C.** AWS Cloudformation
- **D.** AWS Opswork

Explanation :

Answer -A
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.
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 B is invalid since this would mean that the developers need to maintain the EC2 environment
Option C is invalid since this is used for Infrastructure as code
Option D is invalid since this is used to define stacks for your applications and ideally you should use Elastic beanstalk for your docker based development applications
For more information on using Elastic Beanstalk for Docker, 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 30 UNATTEMPTED

Your company has just hit a bottleneck for their on-premise storage and now want to extend their storage to AWS. They want to store the files in S3 and make them available as NFS file shares to their On-premise servers. Which of the following can help achieve this requirement?

- A. Usage of S3 lifecycle policies
- B. Usage of the EFS file system
- C. Usage of the File gateway ✔
- D. Usage of AWS EBS volumes

Explanation :

Answer – C
The AWS Documentation mentions the following
File Gateway – A file gateway supports a file interface into Amazon Simple Storage Service (Amazon S3) and combines a service and a virtual software appliance. By using this combination, you can store and retrieve objects in Amazon S3 using industry-standard file protocols such as Network File System (NFS) and Server Message Block (SMB). The software appliance, or gateway, is deployed into your on-premises environment as a virtual machine (VM) running on VMware ESXi or Microsoft Hyper-V hypervisor. The gateway provides access to objects in S3 as files or file share mount points.
Option A is invalid because this used to transition objects from S3 Standard storage to other storage options.
Option B is invalid because this used while this can be used as a file system, you would still use the File Storage gateway to expose your S3 objects as files
Option D is invalid because this used for storage on EC2 Instances
For more information on what is the Storage gateway, please refer to the below URL

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

Ask our Experts

QUESTION 31 UNATTEMPTED

Your development team have started using the ElastiCache service. You've setup a Memcached cluster for them. After continuous usage, there are alerts being triggered of high utilization for the cluster. Which of the following can be done to resolve the issue of high CPU utilization? Choose 2 answers from the options given below.

- [ ] **A.** Use a larger cache node type ✔
- [ ] **B.** Add more cache nodes ✔
- [ ] **C.** Add Autoscaling to the nodes
- [ ] **D.** Add an Elastic Load balancer in front of the cache cluster

Explanation :

Answer – A and B
This is clearly mentioned in the AWS Documentation

Which Metrics Should I Monitor?

The following CloudWatch metrics offer good insight into ElastiCache performance. In most cases, we recommend that you set CloudWatch alarms for these metrics so that you can take corrective action before performance issues occur.

Metrics to Monitor

- CPUUtilization
- SwapUsage
- Evictions
- CurrConnections

CPUUtilization

This is a host-level metric reported as a percent. For more information, see Host-Level Metrics.

Because Memcached is multi-threaded, this metric can be as high as 90%. If you exceed this threshold, scale your cache cluster up by using a larger cache node type, or scale out by adding more cache nodes.

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

For more information on monitoring your cache cluster, please refer to the below URL

- https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/CacheMetrics.WhichShouldIMonitor.html

(https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/CacheMetrics.WhichShouldIMonitor.html)

Ask our Experts

QUESTION 32 UNATTEMPTED

Your company has a set of EC2 Instances and also servers in their on-premise environment. The configuration management team wants to collect information on these servers such as the software's installed, so that they can record it in their configuration management database. How could you achieve this in the easiest way possible?

- A. Use the AWS Config tool to get the configuration of all the servers
- B. Use the AWS Systems Manager to get the software inventory on the servers ✔
- C. Use the EC2 dashboard to get the configuration of all the servers
- D. Use Amazon Cloudwatch to get the configuration of all the servers

Explanation :

Answer – B
The AWS Documentation mentions the following
You can use AWS Systems Manager Inventory to collect operating system (OS), application, and instance metadata from your Amazon EC2 instances and your on-premises servers or virtual machines (VMs) in your hybrid environment. You can query the metadata to quickly understand which instances are running the software and configurations required by your software policy, and which instances need to be updated.
Option A is invalid because this can check for the configuration changes in resources , but not get information on the actual software's installed on the servers
Option C is invalid because the dashboard does not have this information available
Option D is invalid because you can get logs and metrics from Cloudwatch but not get the list of software's installed
For more information on the Systems Manager inventory, please refer to the below URL

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

Ask our Experts

QUESTION 33 UNATTEMPTED

One of instances recently has an impaired status, and you had to manually recover the instance to ensure it goes back to its original status. What can you do to automate so that in the future if the instance does go back in the impaired state, it can be recovered automatically.

- **A.** Check the Cloudtrail logs and add an alarm action to recover the Instance
- **B.** Create a Cloudwatch alarm and based on the alarm create an action to recover the Instance ✔
- **C.** Create an AWS config rule that triggers an alarm action to recover the instance.
- **D.** Create an AWS Trusted Advisor rule that triggers an alarm and based on that alarm create an action to recover the instance.

Explanation :

Answer – B
You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance. If the instance becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair, you can automatically recover the instance. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata.
Option A is incorrect since this is used to monitor API activity
Option C is incorrect since this is used to check for configuration changes
Option D is incorrect since this is used to check for recommendations
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 34 UNATTEMPTED

You are the Systems Administrator for a company. They have set up an EC2 Instance in a VPC (CIDR 10.0.0.0/16) that is hosting a Web based application. You need to modify the security rules so that the users from around the world can access the application. Also, you need to be able to SSH into the instance from your workstation which has an IP of 20.90.6.7. Which of the following Security rules would you put in place. Choose 2 answers from the options given below.

- [ ] **A.** Add an Inbound Security Rule of port(80) and Source IP as 10.0.0.0/16
- [ ] **B.** Add an Inbound Security Rule of port(80) and Source IP as 0.0.0.0/0 ✔
- [ ] **C.** Add an Inbound Security Rule of port(22) and Source IP as 0.0.0.0/0
- [ ] **D.** Add an Inbound Security Rule of port(22) and Source IP as 20.90.6.7/32 ✔

Explanation :

Answer – B and D
Such as example is also mentioned in the AWS Documentation

Inbound rules		
Protocol type	**Port number**	**Source IP**
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
ICMP	All	0.0.0.0/0
Outbound rules		
Protocol type	**Port number**	**Destination IP**
All	All	0.0.0.0/0

So here you need to ensure that since users from all over the world need access to the web application, the source IP range needs to be 0.0.0.0/0 and not 10.0.0.0/16

And if you want to SSH into the instance from an IP it needs to be 20.90.6.7/32 and not the internet
For more information on using Network Security, please refer to the below URL

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

Ask our Experts

QUESTION 35 UNATTEMPTED

Your company currently has an application that is making use of an instance of AWS RDS MySQL. The application is going to get a new reporting module. The users would prefer that the primary database does not get overloaded due to the high number of queries from the reporting module. Which of the following can be done to fulfil this requirement?

- A. Enable global tables
- B. Enable Multi-AZ
- C. Create a Read Replica ✔
- D. Increase the throughput on the underlying tables

Explanation :

Answer – C
The AWS Documentation clearly gives the advantages of creating Read Replica's
Deploying one or more Read Replicas for a given source DB instance might make sense in a variety of scenarios, including the following:

· Scaling beyond the compute or I/O capacity of a single DB instance for read-heavy database workloads. You can direct this excess read traffic to one or more Read Replicas.

· Serving read traffic while the source DB instance is unavailable. If your source DB instance can't take I/O requests (for example, due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your Read Replicas. For this use case, keep in mind that the data on the Read Replica might be "stale" because the source DB instance is unavailable.

· Business reporting or data warehousing scenarios where you might want business reporting queries to run against a Read Replica, rather than your primary, production DB instance.

· Implementing disaster recovery. You can use promote a Read Replica to a standalone instances as a

disaster recovery solution if the source DB instance fails.

Options A and D are incorrect since these are features of DynamoDB
Option B is incorrect since this is used for high availability of the database
For more information on Read Replica's, please refer to the below URL

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

Ask our Experts

QUESTION 36 UNATTEMPTED

A company has a set of DynamoDB tables. The company wants to ensure that DynamoDB tables are protected and recoverable in case of accidental write or delete operations. Which of the following can be used to fulfil this requirement?

- A. Enable global tables
- B. Use the Point-in-time recovery feature ✔
- C. Enable Autoscaling
- D. Enable Multi-AZ

Explanation :

Answer – B
The AWS Documentation mentions the following
You can enable point-in-time recovery as well as create on-demand backups for your Amazon DynamoDB tables.
Point-in-time recovery helps protect your Amazon DynamoDB tables from accidental write or delete operations. With point in time recovery, you don't have to worry about creating, maintaining, or scheduling on-demand backups. For example, suppose that a test script writes accidentally to a production DynamoDB table. With point-in-time recovery, you can restore that table to any point in time during the last 35 days. DynamoDB maintains incremental backups of your table.
Option A is incorrect since this feature is used if you want the table to be available in another region
Option C is incorrect since if you want to automatically increase the throughput on the tables
Option D is incorrect since this is feature of AWS RDS
For more information on point in time recovery for DynamoDB, please refer to the below URL

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

Ask our Experts

QUESTION 37 UNATTEMPTED

Your company has just setup a set of DynamoDB tables. They need monitoring reports to be made available on how much Read and Write Capacity is being utilized. This would help to get a good idea on how much the tables are being utilized. How can you accomplish this?

- **A.** Use Cloudwatch logs to see the amount of Read and Write Capacity being utilized
- **B.** Use Cloudwatch metrics to see the amount of Read and Write Capacity being utilized ✔
- **C.** Use Cloudtrail logs to see the amount of Read and Write Capacity being utilized
- **D.** Use AWS Config logs see the amount of Read and Write Capacity being utilized

Explanation :

Answer – B
The below tables shows the metrics available for DynamoDB

How Do I Use Amazon DynamoDB Metrics?

The metrics reported by Amazon DynamoDB provide information that you can analyze in different ways. The following list shows some common uses for the metrics. These are suggestions to get you started, not a comprehensive list.

How can I?	Relevant Metrics
How can I monitor the rate of TTL deletions on my table?	You can monitor `TimeToLiveDeletedItemCount` over the specified time period, to track the rate of TTL deletions on your table. For an example of a server-less application using the `TimeToLiveDeletedItemCount` metric, see Automatically archive items to S3 using DynamoDB Time to Live (TTL) with AWS Lambda and Amazon Kinesis Firehose.
How can I determine how much of my provisioned throughput is being used?	You can monitor `ConsumedReadCapacityUnits` or `ConsumedWriteCapacityUnits` over the specified time period, to track how much of your provisioned throughput is being used.
How can I determine which requests exceed the provisioned throughput limits of a table?	`ThrottledRequests` is incremented by one if any event within a request exceeds a provisioned throughput limit. Then, to gain insight into which event is throttling a request, compare `ThrottledRequests` with the `ReadThrottleEvents` and `WriteThrottleEvents` metrics for the table and its indexes.
How can I determine if any system errors occurred?	You can monitor `SystemErrors` to determine if any requests resulted in a HTTP 500 (server error) code. Typically, this metric should be equal to zero. If it isn't, then you might want to investigate. **Note** You might encounter internal server errors while working with items. These are expected during the lifetime of a table. Any failed requests can be retried immediately.

Option A is incorrect since the logs will not give the consumption of the Read and Write Capacity

Option C is incorrect since cloudtrail is only used for API monitoring
Option D is incorrect since this is only used for configuration management
For more information on monitoring with Cloudwatch, please refer to the below URL

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

Ask our Experts

QUESTION 38 UNATTEMPTED

Your company has an S3 bucket located in the EU region. Based on compliance regulations, the objects now need to be replicated from the bucket onto another region. Which of the following steps as a System Administrator do you need to ensure are in place for replication to take place. Choose 2 answers from the options given below.

- [ ] **A.** The source and destination buckets must have versioning enabled ✔
- [ ] **B.** The source and destination buckets must have encryption enabled
- [ ] **C.** The source and destination buckets must be in different AWS Regions ✔
- [ ] **D.** The source and destination buckets must be in same AWS Region

Explanation :

Answer – A and C
The AWS Documentation mentions the following
Requirements for cross-region replication:

- The source and destination buckets must have versioning enabled.
- The source and destination buckets must be in different AWS Regions.
- Amazon S3 must have permissions to replicate objects from that source bucket to the destination bucket on your behalf.

Option B is incorrect since you don't need to have encryption enabled
Option D is incorrect since the buckets need to be in different regions
For more information on cross region replication, please refer to the below URL

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

Ask our Experts

QUESTION 39 UNATTEMPTED

Your company currently has 2 accounts, one is a development AWS account and the other account is used for hosting production-based resources. There's a "Dev" Group in the development account whose users are basically developers who push code from development to the production environment. At times developers might require limited access to the production account. You need to ensure that when an update to an application needs to be made to the production environment, it can be done in the most secure way possible. Which of the following is one of the ways in which this can be managed?

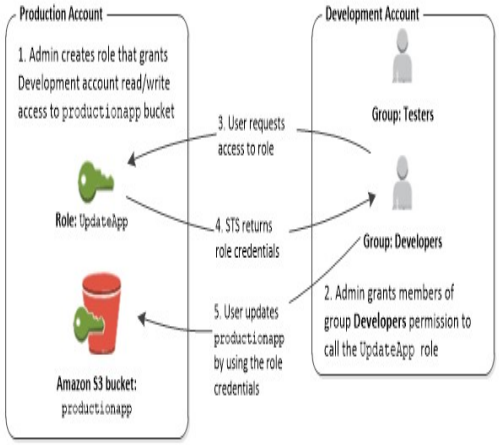
- **A.** Create an IAM user in the production AWS account and share the password for the console access
- **B.** Create an IAM user in the production AWS account and share the access keys
- **C.** Create an IAM user in the production AWS account and share the access keys and ensure the IAM user is part of a secure group
- **D.** Create a cross account role and share the ARN for the role ✔

Explanation :

Answer – D
The AWS Documentation explains this sort of scenario

Example Scenario Using Separate Development and Production Accounts

Imagine that your organization has multiple AWS accounts to isolate a development environment from a production environment. Users in the development account might occasionally need to access resources in the production account. For example, you might need cross-account access when you are promoting an update from the development environment to the production environment. Although you could create separate identities (and passwords) for users who work in both accounts, managing credentials for multiple accounts makes identity management difficult. In the following figure, all users are managed in the development account, but some developers require limited access to the production account. The development account has two groups: Testers and Developers, and each group has its own policy.



All other options are invalid since sharing user details is not the secure way for this sort of access

For more information on common scenarios for cross account access, please refer to the below URL

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html)

Ask our Experts

QUESTION 40 UNATTEMPTED

Your company has an on-premise web server. The company wants to implement a health check system to continuously check the health of the on-premise server. If the health degrades for any reason, then a switch over must be done to a static web site hosted in AWS. Which of the following can be implemented to fulfil this requirement?

- **A.** Use an Elastic Load balancer to divert traffic when the on-premise web server has issues
- **B.** Use Route 53 health checks to failover to the secondary site if the on-premise web server has issues ✔
- **C.** Use Elastic Beanstalk to check for issues in the on-premise web server and then failover to an environment defines in Elastic Beanstalk
- **D.** Use AWS Opsworks to check for issues in the on-premise web server and then failover to an environment defines in AWS Opsworks

Explanation :

Answer – B
The AWS Documentation mentions the following
Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.
Option A is incorrect because this service cannot be used to divert traffic in such a way
Options C and D are incorrect since these services don't have these sort of features
For more information on DNS failover types, please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html)

Ask our Experts

QUESTION 41 UNATTEMPTED

Your company currently has a set of Images that are placed in an S3 bucket. To give better user experience to uses across the world, you have created a Cloudfront distribution with the S3 bucket as the origin. But in your monitoring reports, you now see that a lot of users are bypassing the Cloudfront URL and directly going to the S3 bucket and downloading the images. Which of the following steps can be performed to remediate this issue. Choose 2 answers from the options given below.

- [ ] **A.** Create a Cloudfront origin access identity ✔
- [ ] **B.** Create a separate IAM user
- [ ] **C.** Ensure that only the Cloudfront origin access identity has access to read objects from the S3 bucket. ✔
- [ ] **D.** Ensure that only the IAM user has access to read objects from the S3 bucket.

Explanation :

Answer – A and C
The AWS Documentation mentions the following
To ensure that your users access your objects using only CloudFront URLs, regardless of whether the URLs are signed, perform the following tasks:
1. Create an origin access identity, which is a special CloudFront user, and associate the origin access identity with your distribution. (For web distributions, you associate the origin access identity with origins, so you can secure all or just some of your Amazon S3 content.) You can also create an origin access identity and add it to your distribution when you create the distribution.
2. Change the permissions either on your Amazon S3 bucket or on the objects in your bucket so only the origin access identity has read permission (or read and download permission). When your users access your Amazon S3 objects through CloudFront, the CloudFront origin access identity gets the objects on behalf of your users. If your users request objects directly by using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't.
Options B and D are incorrect since you need to create a Cloudfront origin access identity and not an IAM user
For more information on private content for S3, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html)

Ask our Experts

QUESTION 42 UNATTEMPTED

Your company has a set of EC2 Instances in a private subnet (10.0.1.0/24). These EC2 Instances now need to download updates via HTTPS from the Internet. You setup a NAT instance in the public subnet. Which of the following needs to be added as an incoming rule to the Security group for the NAT instance

- A. Allow Incoming from Source 0.0.0.0/0 on port 80
- B. Allow Incoming from Source 10.0.1.0/24 on port 80
- C. Allow Incoming from Source 0.0.0.0/0 on port 443
- D. Allow Incoming from Source 10.0.1.0/24 on port 443 ✔

Explanation :

Answer - D
The AWS Documentation below provides the recommended rules for the NAT Instance Security groups

NATSG: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comments
10.0.1.0/24	TCP	80	Allow inbound HTTP traffic from servers in the private subnet
10.0.1.0/24	TCP	443	Allow inbound HTTPS traffic from servers in the private subnet
Public IP address range of your home network	TCP	22	Allow inbound SSH access to the NAT instance from your home network (over the Internet gateway)
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet

Option C is incorrect since the incoming requests should come from the Instances in the private subnet

Options A and B are incorrect since the question mentions HTTPS , that means it needs to be allowed on port 443
For more information on the NAT Instance, please refer to the below URL

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

Ask our Experts

QUESTION 43 UNATTEMPTED

You are planning on setting up an application in AWS. This application will be hosting a general-purpose workload application. You want to setup a cost-effective Instance type but also have the ability to be flexible for spikes in application usage. Which of the following can be used to implement this requirement? Choose 2 answers from the options given below.

- [x] **A.** Configure a t2.micro instance ✔
- [ ] **B.** Configure an c4.large instance
- [ ] **C.** Configure burstable performance on the instance
- [x] **D.** Configure the t2 unlimited option ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following
T2 Unlimited is a configuration option for T2 instances that can be set at launch, or enabled at any time for a running or stopped T2 instance.
T2 Unlimited instances can burst above the baseline for as long as required. This enables you to enjoy the low T2 instance hourly price for a wide variety of general-purpose applications, and ensures that your instances are never held to the baseline performance. ?The basic T2 hourly instance price automatically covers all CPU usage spikes if the average CPU utilization of a T2 Unlimited instance over a rolling 24-hour period is at or below the baseline. For a vast majority of general-purpose workloads, T2 Unlimited instances provide ample performance without any additional charges
Option B is invalid since this will not be a cost-effective option
Option C is invalid since this is not a configurable option
For more information on T2 unlimited, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/t2-unlimited.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/t2-unlimited.html)

Ask our Experts

QUESTION 44 UNATTEMPTED

Your company is planning on hosting a batch processing application on a set of EC2 Instances. You need to spin up the Instances for hosting the application. Which of the following would you use as the underlying Instance type for the Instances?

- A. General Purpose
- B. Memory Optimized
- C. Storage Optimized
- D. Compute Optimized ✔

Explanation :

Answer - D
This is mentioned in the AWS Documentation
Compute optimized instances are ideal for compute-bound applications that benefit from high-performance processors. They are well suited for the following applications:

- Batch processing workloads
- Media transcoding
- High-performance web servers
- High-performance computing (HPC)
- Scientific modeling
- Dedicated gaming servers and ad serving engines
- Machine learning inference and other compute-intensive applications

Since the documentation mentions this clearly , all other options are invalid
For more information on Compute Optimized Instances, please refer to the below URL

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

Ask our Experts

QUESTION 45 UNATTEMPTED

Your company has a set of Instances that are located in the EU Region. They need these instances to be available in another region for disaster recovery purposes. How would you accomplish this? Choose 2 answers from the options given below?

- ☐ **A.** Copy the underlying EBS volume to the destination region
- ☐ **B.** Copy the underlying EC2 Instance to the destination region
- ☐ **C.** Make an AMI of the EC2 Instance ✔
- ☐ **D.** Copy the AMI to the destination region ✔

Explanation :

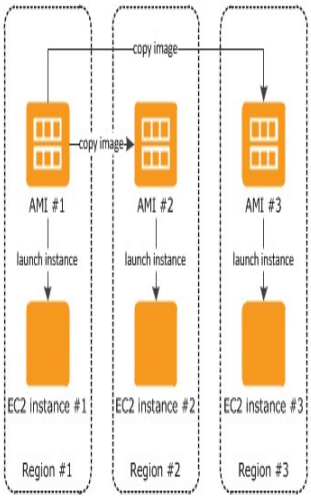
Answer – C and D
This is mentioned in the AWS Documentation

Cross-Region AMI Copy

Copying an AMI across geographically diverse regions provides the following benefits:

- Consistent global deployment: Copying an AMI from one region to another enables you to launch consistent instances in different regions based on the same AMI.
- Scalability: You can more easily design and build global applications that meet the needs of your users, regardless of their location.
- Performance: You can increase performance by distributing your application, as well as locating critical components of your application in closer proximity to your users. You can also take advantage of region-specific features, such as instance types or other AWS services.
- High availability: You can design and deploy applications across AWS regions, to increase availability.

The following diagram shows the relations among a source AMI and two copied AMIs in different regions, as well as the EC2 instances launched from each. When you launch an instance from an AMI, it resides in the same region where the AMI resides. If you make changes to the source AMI and want those changes to be reflected in the AMIs in the target regions, you must recopy the source AMI to the target regions.



Options A and B are invalid because you can't directly copy EC2 Instances and EBS volumes to other regions

For more information on copying AMI's, please refer to the below URL

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

Ask our Experts

QUESTION 46 UNATTEMPTED

You are the Systems Administrator for a company. You have been instructed to create a VPC setup which has a public and private subnet. The public subnet needs to have a NAT gateway which will be used to route traffic to the Internet for Instances in the private subnet. Which of the following routing entries would you create in the respective main and custom route tables? Choose 2 answers from the options given below

- [ ] **A.** In the main route table add a route with destination of 0.0.0.0/0 and the NAT gateway ID ✔
- [ ] **B.** In the main route table add a route with destination of 0.0.0.0/0 and the Internet gateway ID
- [ ] **C.** In the custom route table add a route with destination of 0.0.0.0/0 and the NAT gateway ID
- [ ] **D.** In the custom route table add a route with destination of 0.0.0.0/0 and the Internet gateway ID ✔

Explanation :

Answer – A and D
This is mentioned in the AWS Documentation

Main Route Table

The first entry is the default entry for local routing in the VPC; this entry enables the instances in the VPC to communicate with each other. The second entry sends all other subnet traffic to the NAT gateway (for example, `nat-12345678901234567`).

Destination	Target
`10.0.0.0/16`	local
`0.0.0.0/0`	*nat-gateway-id*

Custom Route Table

The first entry is the default entry for local routing in the VPC; this entry enables the instances in this VPC to communicate with each other. The second entry routes all other subnet traffic to the Internet over the Internet gateway (for example, `igw-1a2b3d4d`).

Destination	Target
`10.0.0.0/16`	local
`0.0.0.0/0`	*igw-id*

Options B and C are invalid because of the configurations mentioned in the Route Tables
For more information on the settings for the VPC with the public and private subnets, please refer to the below URL

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

Note:

"main route table corresponds to the public subnet" is practically **NOT** recommended in a production setup in the industry from the sucurity point of view.

Keeping in mind the best security practices, we should not have a way out to the internet from our Main Route Table.

This is because every single time we create a new subnet it's going to be associated by default with the Main Route Table. Or it can be rephrased as, when a subnet has not been associated with any Route Table it is going to be associated with the Main Route Table. So, if the Main Route Table has a route out to the internet, every subnet which is not explicitly attached with any Route Table is public by default which is risky.

Keeping the above statements in mind, the following is documented by AWS as a best practice:

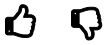
A **custom route table** should be associated with the **public subnet**. This route table contains an entry that enables instances in the subnet to communicate with other instances in the VPC over IPv4, and an entry that enables instances in the subnet to communicate directly with the Internet over IPv4.

The **main route table** should be associated with the **private subnet**. The route table contains an entry that enables instances in the subnet to communicate with other instances in the VPC over IPv4, and an entry that enables instances in the subnet to communicate with the Internet through the NAT gateway over IPv4.

That's the reason the question has not explicitly mentioned about which Route Table is associated with the Public/Private subnet.
AWS Docs Reference

- 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 47 UNATTEMPTED

You are currently managing an AWS RDS instance for your company. You need to be notified whenever the backup occurs for the AWS RDS database. How can you accomplish this in the easiest way possible? Choose 2 answers from the options given below

☐ **A.** Subscribe to AWS RDS Events service ✔

- [ ] **B.** Create an SQS queue for the event messages
- [x] **C.** Create an SNS topic ✔
- [ ] **D.** Add a Lambda trigger to the AWS RDS database

Explanation :

Answer – A and C
This is mentioned in the AWS Documentation
Amazon RDS groups these events into categories that you can subscribe to so that you can be notified when an event in that category occurs. You can subscribe to an event category for a DB instance, DB cluster, DB snapshot, DB cluster snapshot, DB security group, or for a DB parameter group. For example, if you subscribe to the Backup category for a given DB instance, you will be notified whenever a backup-related event occurs that affects the DB instance. If you subscribe to a Configuration Change category for a DB security group, you will be notified when the DB security group is changed. You will also receive notification when an event notification subscription changes.
Option B is invalid because SQS is used as the messaging service. You need to use SNS topics for notifications
Option D is invalid because you need to subscribe to AWS RDS events
For more information on database events, please refer to the below URL

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

Ask our Experts

QUESTION 48 UNATTEMPTED

Your company has set a Network Load Balancer in AWS. They need to get the detailed traffic requests that flow into the load balancer. Which of the following can help accomplish this requirement?

- [ ] **A.** Use Cloudwatch Logs
- [ ] **B.** Use Cloudwatch metrics
- [ ] **C.** Use Cloudtrail logs
- [x] **D.** Use VPC Flow Logs ✔

Explanation :

Answer – D
This is mentioned in the AWS Documentation
You can use VPC Flow Logs to capture detailed information about the traffic going to and from your Network Load Balancer.
Create a flow log for each network interface for your load balancer. There is one network interface per load balancer subnet. To identify the network interfaces for a Network Load Balancer, look for the name of the load balancer in the description field of the network interface.
Option A is incorrect since here you will not get the detailed traffic information for the Network Load balancer.
Option B is incorrect since this service is used to retrieve statistics about data points for your load balancers
Option C is incorrect since this service is used for API logging
For more information on monitoring the Network Load Balancer, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-monitoring.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-monitoring.html)

Ask our Experts

QUESTION 49 UNATTEMPTED

Your company has a Redshift cluster available in the EU region. They need to ensure that the cluster is available in another region in case any issues occur in the primary region. Which of the following can be used to accomplish this requirement?

- A. Enable Multi-AZ for the Redshift cluster
- B. Copy a snapshot of the cluster to another region ✔
- C. Enable global tables for the Redshift cluster
- D. Enable Read Replica's for the Redshift cluster

Explanation :

Answer – B

You can configure Amazon Redshift to automatically copy snapshots (automated or manual) for a cluster to another region. When a snapshot is created in the cluster's primary region, it will be copied to a secondary region; these are known respectively as the *source region* and *destination region*. By storing a copy of your snapshots in another region, you have the ability to restore your cluster from recent data if anything affects the primary region.
Options A and D are invalid because these are options associated with AWS RDS
Option C is invalid since this is an option available with DynamoDB
For more information on working with snapshots in Redshift, please refer to the below URL

- https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html (https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html)

Ask our Experts

QUESTION 50 UNATTEMPTED

You work in a company as a Systems administrator. Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws. Which of the following can be done to ensure this? Choose 2 answers from the options given below.

- [ ] **A.** Use AWS Config to ensure that the servers have no critical flaws.
- [ ] **B.** Use AWS Inspector to ensure that the servers have no critical flaws. ✔
- [ ] **C.** Use AWS Inspector to patch the servers
- [ ] **D.** Use AWS SSM to patch the servers ✔

Explanation :

Answer – B and D
The AWS Documentation mentions the following on AWS Inspector
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.
Once you understand the list of servers which require critical updates , you can rectify them by installing

the required patches via the SSM tool.
Option A is invalid because the AWS Config service is not used to check the vulnerabilities on servers
Option C is invalid because the AWS Inspector service is not used to patch servers
For more information on AWS Inspector, please visit the following URL

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

For more information on the Systems Manager, please visit the following URL

- https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html (https://docs.aws.amazon.com/systems-manager/latest/APIReference/Welcome.html)

Ask our Experts

QUESTION 51 UNATTEMPTED SECURITY AND COMPLIANCE

A user has created a VPC with public and private subnets. The VPC has CIDR 10.0.0.0/16. The private subnet uses CIDR 10.0.1.0/24 and the public subnet uses CIDR 10.0.2.0/24. The user is planning to host a web server in the public subnet on port 80. And a database server in the private subnet on port 3306. The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?

- ☐ **A.** For Inbound allow Source: 10.0.1.0/24 on port 80 ✔
- ☐ **B.** For Outbound allow Destination: 0.0.0.0/0 on port 80
- ☐ **C.** For Inbound allow Source: 10.0.2.0/24 on port 80 ✔
- ☐ **D.** For Outbound allow Destination: 0.0.0.0/0 on port 443

Explanation :

Answer – A and C

- The requests to the web server will not be routed via the NAT instance, so you don't need to allow traffic from the web server. The NAT instance is only required for the database in the private subnet

The AWS Documentation gives an example on this

NATSG: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comments
10.0.1.0/24	TCP	80	Allow inbound HTTP traffic from servers in the private subnet
10.0.1.0/24	TCP	443	Allow inbound HTTPS traffic from servers in the private subnet
Public IP address range of your home network	TCP	22	Allow inbound SSH access to the NAT instance from your home network (over the Internet gateway)
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet

Based on the above, all other options are invalid

- The option A is also not required because NAT will work only if the traffic originates internally first. If the traffic is coming from outside, it will not be forwarded to the destination.
- For more information on security groups for NAT Instances, please visit the following URL
  - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html)

Note:
For this question, we have to select the incorrect response i.e **"**Which of the below-mentioned entries is **not required f**or the NAT security group?**".** So based on this provided options are correct.

Ask our Experts

QUESTION 52 **UNATTEMPTED**

Your team is currently using an EC2 Instance which used General Purpose SSD Volumes. The Instance is hosting a database software. At times throughout the day you are seeing a lot of wait time on the disk volume that the database's data is stored on. Which of the following can be used to alleviate the issue?

- A. Consider moving the database to the DynamoDB service
- B. Consider using Provisioned IOPS as the underlying EBS volume ✔
- C. Consider placing an Elastic Load balancer in front of the database
- D. Consider moving the database to the Redshift service

Explanation :

Answer – B
Provisioned IOPS is better for database workloads as also mentioned in the AWS Documentation

	Solid-State Drives (SSD)		Hard disk Drives (HDD)	
Volume Type	General Purpose SSD (gp2)*	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use Cases	• 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: o MongoDB o Cassandra o Microsoft SQL Server o MySQL o PostgreSQL o 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

Options A and D are incorrect since the question does not mention the type of data being stored for us to make a decision what would be the ideal underlying service to host the data

Option C is incorrect since this would not help solve the issue
For more information on EBS volume types, please visit the following URL

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

Ask our Experts

QUESTION 53 UNATTEMPTED

You are deploying several Cloudformation templates. Whilst deploying the templates, you are getting the below error.

Sender
Throttling
Rate exceeded

Which of the following can be done to resolve the issue?

- **A.** Add a pause in the Cloudformation templates
- **B.** Add an exponential backoff between the calls to the createStack API ✔
- **C.** Use a large instance from where the cloudformation template is being deployed
- **D.** Combine the stacks into one template and deploy the stack.

Explanation :

Answer – B
The error is happening because the create stack API is creating too many resources at the same time.
You can add some delayed between the requests using a concept called exponential backoff
Option A is invalid since you cannot add a pause, you can add wait or dependency conditions in Cloudformtion
Option C is invalid because using a large instance will not help, because this an issue with the number of requests being fired against Cloudformation
Option D is invalid because using one larger template will just make the situation worse
For more information on exponential backoff, please visit the following url

- https://forums.aws.amazon.com/thread.jspa?threadID=100414 (https://forums.aws.amazon.com/thread.jspa?threadID=100414)

Ask our Experts

QUESTION 54 UNATTEMPTED

A software development company is currently working on developing a new application. This will be hosted in AWS. In order to test the application, a performance test is being conducted. The only issue is that whenever the infrastructure needs to be scaled, the team needs to go to the IT admin team to request for new infrastructure. How can you automate such requests? Choose 2 options

- [x] **A.** Create an Autoscaling Group and Launch configuration ✔
- [x] **B.** Ensure the Autoscaling Group creates new instances based on instance utilization. ✔
- [ ] **C.** Create an Elastic Load Balancer
- [ ] **D.** Create a target group in the load balancer

Explanation :

Answer – A and B
The AWS Documentation mentions the following
When you configure dynamic scaling, you must define how you want to scale in response to changing demand. For example, you have a web application that currently runs on two instances and you do not want the CPU utilization of the Auto Scaling group to exceed 70 percent. You can configure your Auto Scaling group to scale automatically to meet this need. The policy type determines how the scaling action is performed.
Options C and D are in correct because in this case , you need to use the Autoscaling service
For more information on Dynamic scaling, please visit the following url

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html)

Ask our Experts

QUESTION 55 UNATTEMPTED

An Audit company is currently carrying out an audit of your infrastructure. They want to know what the types of security procedures are implemented at the data centres that host the AWS resources. Which of the following would you carry out to fulfil this requirement?

- A. Raise a call with AWS Support to get a tour of the data centre.
- B. Send a copy of the AWS Security Whitepapers
- C. Contact an AWS Direct Connect partner
- D. Use a document from the AWS Artifact web service ✔

Explanation :

Answer – D
AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as *audit artifacts*) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls
Because of what the AWS Documentation mentions , all other options are invalid
For more information on AWS Artifact, please visit the following url

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

Ask our Experts

QUESTION 56 UNATTEMPTED

Your team has just deployed an application to production. The application consists of a web server hosted on an EC2 Instance and a MySQL database hosted using the Relational database service. After a period of ten days, one of the core application

tables has been dropped by accident and needs to be retrieved immediately. Which of the following Amazon RDS feature allows you to reliably restore your database within 5 minutes of when the deletion occurred.

- A. Multi-AZ RDS
- B. RDS Snapshots
- C. RDS Read Replica's
- D. RDS Automated Backup ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Amazon RDS creates and saves automated backups of your DB instance. Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Amazon RDS creates automated backups of your DB instance during the backup window of your DB instance. Amazon RDS saves the automated backups of your DB instance according to the backup retention period that you specify. If necessary, you can recover your database to any point in time during the backup retention period.
Option A is invalid since this is used to achieve high availability for the database
Option B is invalid since this is used to take a snapshot of the database at a particular point in time
Option C is invalid since this is used for offloading the reads off the primary database
For more information on automated backups, please visit the following url

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

Ask our Experts

QUESTION 57 UNATTEMPTED

Your team needs a set of EC2 Instances setup in a VPC. The primary requirement of this instance is that it needs to support higher bandwidth and higher packet per second (PPS) performance. Which of the following option would you consider for this requirement?

- A. Consider using placement groups
- B. Use EBS Optimized Instance types
- C. Use Instance types which support Enhanced Networking ✔
- D. Consider using Elastic IP addresses

Explanation :

Answer – C
The AWS Documentation mentions the following
Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html#supported_instances). SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. There is no additional charge for using enhanced networking.
Option A is invalid since this is used for high throughput between Instances
Option B is invalid since this is used for better performance for EBS volumes
Option D is invalid since this is used for static IP addressing
For more information on Enhanced Networking, please visit the following url

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

Ask our Experts

QUESTION 58 UNATTEMPTED

Your company uses S3 to store critical data for your company. Several users within your group currently have full permissions to your S3 buckets. You need to come up with a solution that does not impact your users and also protect against the accidental deletion of objects. Which two options will address this issue? Choose 2 answers from the options given below

- A. Enable versioning on your S3 Buckets ✔

- [ ] **B.** Configure your S3 Buckets with MFA delete ✔
- [ ] **C.** Create a Bucket policy and only allow read only permissions to all users at the bucket level
- [ ] **D.** Enable object life cycle policies and configure the data older than 3 months to be archived in Glacier

Explanation :

Answer – A and B

The AWS Documentation mentions the following
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.
You can optionally add another layer of security by configuring a bucket to enable MFA (multi-factor authentication) Delete, which requires additional authentication for either of the following operations:

- Change the versioning state of your bucket
- Permanently delete an object version

Option C is invalid since using the bucket policy could affect the access level

Option D is invalid since using the lifecycle policy is not the solution for this issue

For more information on Versioning and MFA delete, please visit the following URL

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

Ask our Experts

QUESTION 59 UNATTEMPTED

Your team currently has an Autoscaling Group defined in AWS which is used to dynamically manage the EC2 Instances for an application. Currently there are some issues in the application and for a brief moment in time, the team needs to debug what is the issue. What can be done to ensure that this request can be fulfilled?

- **A.** Delete the Autoscaling Group so that you can carry out the investigation on the underlying Instances
- **B.** Delete the Launch Configuration so that you can carry out the investigation on the underlying Instances
- **C.** Suspend the scaling process so that you can carry out the investigation on the underlying Instances ✔
- **D.** Use the AWS Config to take a configuration snapshot of the Instances and then carry out the investigation on the underlying Instances

Explanation :

Answer – C
The AWS Documentation mentions the following
You can suspend and then resume one or more of the scaling processes for your Auto Scaling group. This can be useful when you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without invoking the scaling processes.
Amazon EC2 Auto Scaling can suspend processes for Auto Scaling groups that repeatedly fail to launch instances. This is known as an *administrative suspension*, and most commonly applies to Auto Scaling groups that have been trying to launch instances for over 24 hours but have not succeeded in launching any instances. You can resume processes suspended for administrative reasons.
Options A and B are invalid since you should not delete either the Autoscaling Group or the Launch Configuration , this will disrupt the architecture of the application
Option D is invalid since this is not possible with the AWS Config service
For more information on suspending and resuming autoscaling processes, please visit the following url

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html)

Ask our Experts

QUESTION 60 UNATTEMPTED

An organization is generating digital policy files which are required by the admins for verification. Once the files are verified they may not be required in the future unless there is some compliance issue. As the Sysops administrator, you have been requested to create a data store in AWS to meet this requirement. Which of the following would be the best COST-effective option for this?

- A. AWS S3 - Reduced Redundancy Storage
- B. AWS S3 - Standard Storage
- C. AWS - RDS
- D. AWS Glacier ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Amazon Glacier is an extremely low-cost storage service that provides durable storage with security features for data archiving and backup. With Amazon Glacier, customers can store their data cost effectively for months, years, or even decades. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations
Options A and B are invalid since these are costlier options than AWS Glacier
Option C is incorrect since this is a relational database service
For more information on Amazon Glacier, please visit the following URL

- https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html (https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html)

Ask our Experts

QUESTION 61 UNATTEMPTED

A company wants to setup a hybrid connection between their AWS VPC and their on-premise network. They need to have high bandwidth and less latency because they need to transfer their current database workloads to AWS. Which of the following would you use for this purpose?

- **A.** AWS Managed software VPN
- **B.** AWS Managed hardware VPN
- **C.** AWS Direct Connect ✔
- **D.** AWS VPC Peering

Explanation :

Answer – C
The AWS Documentation mentions the following
AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
Options A and B are incorrect since using a VPN will not give you high bandwidth network connections
Option D is incorrect since this is used to connect multiple VPC's together
For more information on AWS Direct Connect, please visit the following URL

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

Ask our Experts

QUESTION 62 UNATTEMPTED

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

- A. AWS Elastic Beanstalk ✔
- B. AWS Cloudfront
- C. AWS Cloudformation
- D. AWS Opswork

Explanation :

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

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

Hence, A is the CORRECT answer.

Option B is incorrect since this a content delivery service

Option C is incorrect here. Because we have a template in AWS Elastic Beanstalk for LAMP.
Although Cloud formation can also perform the same requirement of the scenario it would be easier to deploy the software using ElasticBeanstalk environment rather than Cloud formation templates.

For more information on launching a LAMP stack with Elastic Beanstalk:

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

Option D is incorrect since this is best used when you want to use configuration management tools such as Puppet or Chef
For more information on AWS Cloudformation, please visit the following URL

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

Ask our Experts

QUESTION 63 UNATTEMPTED

A set of developers want to query some data from a set of CSV files which are stored in S3. They don't want to develop a specific program for this and want to use any AWS service if possible. Which of the following could you use for this requirement?

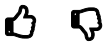
- A. AWS Athena ✔
- B. AWS Redshift
- C. AWS DynamoDB
- D. AWS Glacier

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.
Option B is incorrect since this service is used as Data warehousing solution
Option C is incorrect since this is used a NoSQL database solution
Option D is incorrect since this is used for archive storage
For more information on AWS Athena, please visit the following URL

- https://docs.aws.amazon.com/athena/latest/ug/what-is.html (https://docs.aws.amazon.com/athena/latest/ug/what-is.html)

Ask our Experts



QUESTION 64 UNATTEMPTED

Your company is planning on setting up a performance-sensitive workload in AWS. You need to setup the EC2 Instances for hosting this workload. Which of the following are some of the ideal configurations that you should look for when setting up the EC2 Instance. Choose 2 answers from the options given below

- [ ] **A.** Ensure to choose an EBS Optimized Instance ✔
- [ ] **B.** Ensure to choose an Instance store Instance type
- [ ] **C.** Ensure to choose an Instance type with 10 Gigabit network connectivity ✔
- [ ] **D.** Ensure to use Cold HDD volumes

Explanation :

Answer – A and C
The AWS Documentation mentions the following
Any performance-sensitive workloads that require minimal variability and dedicated Amazon EC2 to Amazon EBS traffic, such as production databases or business applications, should use volumes that are attached to an EBS-optimized instance or an instance with 10 Gigabit network connectivity. EC2 instances that do not meet this criterion offer no guarantee of network resources. The only way to ensure sustained reliable network bandwidth between your EC2 instance and your EBS volumes is to launch the EC2 instance as EBS-optimized or choose an instance type with 10 Gigabit network connectivity
Option B is incorrect since this is used for temporary storage instances
Option D is incorrect since this is used for archive storage for EC2 Instances
For more information on AWS EBS configuration, please visit the following URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-ec2-config.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-ec2-config.html)

Ask our Experts

QUESTION 65 UNATTEMPTED

A company is planning a disaster recovery procedure for their EBS volumes. This is because of the criticality of the data stored on these volumes. They want to ensure that this process is automated. Which of the following service can you use for the Automation process

- ○ **A.** AWS Lambda ✔
- ○ **B.** AWS API gateway
- ○ **C.** AWS Cloudtrail

D. AWS Config

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon EBS emits notifications based on Amazon CloudWatch Events for a variety of snapshot and encryption status changes. With CloudWatch Events, you can establish rules that trigger programmatic actions in response to a change in snapshot or encryption key state. For example, when a snapshot is created, you can trigger an AWS Lambda function to share the completed snapshot with another account or copy it to another region for disaster-recovery purposes
Option B is invalid since this is used to manage API's
Option C is invalid since this is used for API logging
Option D is invalid since this is used for configuration management
For more information on AWS EBS cloudwatch events, please visit the following URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-cloud-watch-events.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-cloud-watch-events.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14836)

- 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)