NEW PRACTICE TEST V

Attempt	1	**Completed on**	Tuesday , 29 January 2019 , 02:06 PM
Marks Obtained	0 / 65	**Time Taken**	00 H 00 M 37 S
Your score is	0.0%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	65	0	1	64

65 Questions	0 Correct	1 Incorrect	64 Unattempted

Show Answers: All

QUESTION 1 INCORRECT

Your company is planning on move their on-premise MySQL database to an AWS RDS Instance. They want to understand what are the key activities that will be performed by AWS which would reduce the administrative activities of their IT staff. Which of the following is carried out by AWS for database hosted in the AWS RDS? Choose 2 answers from the options given below

- [x] **A.** Create and maintain backups so that you can restore to a point in time recovery of 5 minutes ✔
- [ ] **B.** Create and maintain backups which are specially built for long term retention of 6 months to one year
- [ ] **C.** Installing critical security patches for the database ✔
- [x] **D.** Optimizing database queries fired on the database ✖

Explanation :

Answer – A and C
Option B is incorrect since the maximum retention period possible for RDS databases is 35 days.
Option D is incorrect because query optimization is not at all related to RDS. Query optimization is related specifically to the respective database engine.
Option C is correct because Amazon RDS is a fully managed service. So, under the Shared Responsibility Model AWS will take care of the security patches.
The AWS Documentation mentions the following
Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying operating system (OS) or database engine version.
You can restore a DB instance to a specific point in time, creating a new DB instance. RDS uploads transaction logs for DB instances to Amazon S3 every 5 minutes.
For more information on point in time recovery and maintaining a database, please visit the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.htm (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html)
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIT.html)

Ask our Experts

QUESTION 2 UNATTEMPTED

Your team is working on a set of Instances which are created as t2.small Instance types. Based on the workload, they are now experiencing severe networking issues on the Instance. Which of the following can be done to resolve the issue?

- A. Upgrade the Instance to a larger Instance type ✔
- B. Add an additional ENI to the Instance
- C. Use an EBS Optimized Instance
- D. Change the underlying EBS volume to Provisioned IOPS

Explanation :

Answer – A

Every Instance type has a limitation on its capability. So, if there is an issue in the capability of the Instance from the networking perspective, upgrade to a larger instance type which will provide better networking capabilities.
Option B is incorrect since the network bottleneck is in the Instance
Options C and D are incorrect since working with the EBS volume will not improve the network performance
For more information on Instance types, please visit the below URL

- https://aws.amazon.com/ec2/instance-types/ (https://aws.amazon.com/ec2/instance-types/)

Ask our Experts

QUESTION 3 UNATTEMPTED

Your testing team wants to conduct a series of tests on an environment hosted on a set of EC2 Instances. One of the tests include conducting penetration testing on the underlying instances. Which of the following should be taken into mind when conducting penetration testing?

- **A.** It may be performed by the customer against their own instances, only if performed from EC2 instances.
- **B.** It may be performed by AWS and is periodically performed by AWS.
- **C.** It may be performed by AWS and will be performed by AWS upon customer request.
- **D.** It may be performed by the customer against their own instances with prior authorization from AWS. ✔

Explanation :

Answer – D
The AWS documentation is very strict regarding this policy
Our Acceptable Use Policy (https://aws.amazon.com/aup/) describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. However, because penetration testing and other simulated events are frequently indistinguishable from these activities, we have established a policy for customers to request permission to conduct penetration tests and vulnerability scans to or originating from the AWS environment.
Since the policy is mentioned clearly and there are no deviations from this, all other options are incorrect
For more information on Penetration Testing, please visit the below URL

- https://aws.amazon.com/security/penetration-testing/ (https://aws.amazon.com/security/penetration-testing/)

Ask our Experts

QUESTION 4 UNATTEMPTED

You work as a SysOps Administrator for a company. They have a read intensive MySQL database that needs to be migrated to AWS. They need to ensure high availability for the setup, ensure reads are effectively managed and the infrastructure scales accordingly. Which of the following would you consider? Choose 2 answers from the options given below

- [ ] **A.** Use DynamoDB tables
- [x] **B.** Create AWS Aurora clusters ✔
- [ ] **C.** Use Autoscaling for provisioned throughput for the DynamoDB tables
- [x] **D.** Use Autoscaling for provisioning Aurora Read Replica's based on demand ✔

Explanation :

Answer – B and D
The AWS Documentation mentions the following
To meet your connectivity and workload requirements, Aurora Auto Scaling dynamically adjusts the number of Aurora Replicas provisioned for an Aurora DB cluster. Aurora Auto Scaling enables your Aurora DB cluster to handle sudden increases in connectivity or workload. When the connectivity or workload decreases, Aurora Auto Scaling removes unnecessary Aurora Replicas so that you don't pay for unused provisioned DB instances.
You define and apply a scaling policy to an Aurora DB cluster. The *scaling policy* defines the minimum and maximum number of Aurora Replicas that Aurora Auto Scaling can manage. Based on the policy, Aurora Auto Scaling adjusts the number of Aurora Replicas up or down in response to actual workloads, determined by using Amazon CloudWatch metrics and target values.
Options A and C are incorrect since Aurora is a MySQL compatible database and should be used instead.
For more information on using Autoscaling, please visit the below URL

- https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScaling.html (https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScaling.html)

Ask our Experts

QUESTION 5 UNATTEMPTED

Your company has a set of sensitive documents in an S3 bucket. They want to ensure that only privileged IAM users can access the contents of the bucket using their MFA devices. How can you ensure this sort of access is provided for the bucket? Choose 2 answers from the options given below

- [ ] **A.** Enable versioning on the bucket
- [ ] **B.** Enable MFA delete on the bucket
- [ ] **C.** Ensure MFA is enabled for the privileged IAM users ✔
- [ ] **D.** Ensure a bucket policy is in place to only allow access if users are MFA authenticated ✔

Explanation :

Answer – C and D
The AWS Documentation mentions the following
Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your AWS environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code.
You can enforce the MFA authentication requirement using the aws:MultiFactorAuthAge key in a bucket policy. IAM users can access Amazon S3 resources by using temporary credentials issued by the AWS Security Token Service (STS). You provide the MFA code at the time of the STS request.
Options A and B are incorrect since these are used to ensure users don't accidentally delete objects. But here we want to ensure that users use MFA to access the contents in the bucket.
For more information on example bucket policies, please visit the below URL

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

Ask our Experts

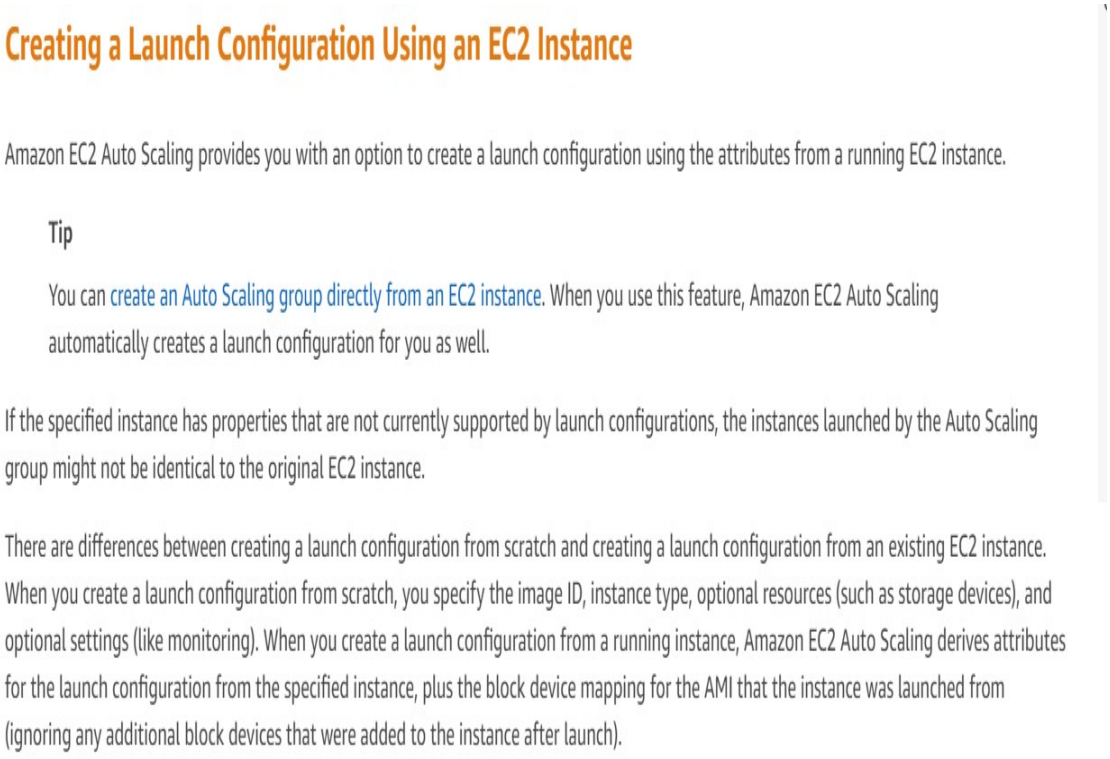
QUESTION 6 UNATTEMPTED

Your company has an EC2 Instance running a web application. They now want to add high availability to the instance. Which of the following is the easiest way to achieve this, ensuring no downtime for the current instance?

- **A.** Create an AMI out of the running instance. Create a new launch configuration and an Autoscaling Group. Terminate the current instance and launch the Autoscaling Group to launch a new instance.
- **B.** Create an Autoscaling Group out of the running EC2 Instance ✔
- **C.** Terminate the instance and launch it via an Elastic Beanstalk environment
- **D.** Terminate the instance and launch it via an Opswork stack

Explanation :

Answer – B
The AWS Documentation mentions the following



Creating a Launch Configuration Using an EC2 Instance

Amazon EC2 Auto Scaling provides you with an option to create a launch configuration using the attributes from a running EC2 instance.

Tip

You can create an Auto Scaling group directly from an EC2 instance. When you use this feature, Amazon EC2 Auto Scaling automatically creates a launch configuration for you as well.

If the specified instance has properties that are not currently supported by launch configurations, the instances launched by the Auto Scaling group might not be identical to the original EC2 instance.

There are differences between creating a launch configuration from scratch and creating a launch configuration from an existing EC2 instance. When you create a launch configuration from scratch, you specify the image ID, instance type, optional resources (such as storage devices), and optional settings (like monitoring). When you create a launch configuration from a running instance, Amazon EC2 Auto Scaling derives attributes for the launch configuration from the specified instance, plus the block device mapping for the AMI that the instance was launched from (ignoring any additional block devices that were added to the instance after launch).

All other options are invalid because it would cause a downtime to the environment

For more information on creating a launch configuration from an existing instance, please visit the below URL

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-lc-with-instanceID.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-lc-with-instanceID.html)

Ask our Experts

QUESTION 7 UNATTEMPTED

You are a SysOps Administrator for a company. The company is planning to start using AWS and launch a set of resources which will consist of EC2 Instances and an RDS Instance. You need to ensure you draft the responsibilities for your team when it comes to the maintenance of the infrastructure on AWS. Which of the following would you consider? Choose 2 answers from the options given below.

- ☐ **A.** Patch management of the underlying physical servers
- ☐ **B.** Patch management of the underlying guest OS ✔
- ☐ **C.** Inventory management for the underlying infrastructure devices
- ☐ **D.** Inventory management for the underlying databases ✔

Explanation :

Answer – B and D
The AWS Documentation mentions the following
Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

Options A and C are incorrect since these are the responsibility of AWS
For more information on the Shared Responsibility Model, please visit the below URL

- https://aws.amazon.com/compliance/shared-responsibility-model/ (https://aws.amazon.com/compliance/shared-responsibility-model/)

Ask our Experts

QUESTION 8 UNATTEMPTED

You are a SysOps Administrator for a company. The company wants to establish the backups of their EBS Volumes. This needs to be done because of the critical data stored on these volumes. Which of the following can be used to accomplish this? Choose 2 answers from the options given below

- [ ] **A.** Create a RAID 0 configuration of multiple volumes
- [ ] **B.** Create a RAID 1 configuration of multiple volumes ✔
- [ ] **C.** Create regular EBS Snapshots of the EBS Volumes ✔
- [ ] **D.** Create regular EBS Volumes copies

Explanation :

Answer – B and C
The AWS Documentation mentions the following
You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are *incremental* backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

Configuration	Use	Advantages	Disadvantages
RAID 0	When I/O performance is more important than fault tolerance; for example, as in a heavily used database (where data replication is already set up separately).	I/O is distributed across the volumes in a stripe. If you add a volume, you get the straight addition of throughput.	Performance of the stripe is limited to the worst performing volume in the set. Loss of a single volume results in a complete data loss for the array.
RAID 1	When fault tolerance is more important than I/O performance; for example, as in a critical application.	Safer from the standpoint of data durability.	Does not provide a write performance improvement; requires more Amazon EC2 to Amazon EBS bandwidth than non-RAID configurations because the data is written to multiple volumes simultaneously.

Option A is incorrect since this is used to increase the IOPS of clubbed volumes

Option D is incorrect since you need to use EBS Snapshots
For more information on EBS Snapshots and RAID Configurations, please visit the below URL's

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

Ask our Experts

QUESTION 9 UNATTEMPTED

Your company has created a set of Cloudformation stacks. These stacks are used to deploy various environments in their AWS account. One of the underlying EC2 Instances needs to be changed and upgraded to a higher Instance type. The EC2 Instance was created as part of the Cloudformation stack. Which of the following is the easiest way to make this change?

- A. Create a new Cloudformation template and deploy it
- B. Create a new Cloudformation template. Delete the older one and deploy the new template
- C. Make changes to the current stack settings ✔
- D. Create a new instance and add it to the stack

Explanation :

Answer - C
The AWS Documentation mentions the following
When you need to make changes to a stack's settings or change its resources, you update the stack instead of deleting it and creating a new stack. For example, if you have a stack with an EC2 instance, you can update the stack to change the instance's AMI ID.
When you update a stack, you submit changes, such as new input parameter values or an updated template. AWS CloudFormation compares the changes you submit with the current state of your stack and updates only the changed resources.
All other options are not the best options to implement for the change.
For more information on updating stacks, please visit the below URL's

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks.html)

Ask our Experts

QUESTION 10 UNATTEMPTED

A company has a set of DynamoDB tables. They have requested you as the SysOps Administrator to ensure that backups are available for the tables for compliance purposes. How can you enable this in the easiest way possible?

- A. Enable on-demand backups for the tables ✔
- B. Create a cron job to copy the data from one table to a backup table
- C. Create EBS snapshots for the volumes holding the data
- D. Enable DAX for the DynamoDB table

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon DynamoDB provides on-demand backup capability. It allows you to create full backups of your tables for long-term retention and archival for regulatory compliance needs. You can back up and restore your DynamoDB table data anytime with a single click in the AWS Management Console or with a single API call. Backup and restore actions execute with zero impact on table performance or availability.
Option B is incorrect since this would not be the ideal approach, too much maintenance would be involved
Option C is incorrect since DynamoDB does not give you access to the underlying infrastructure
Option D is incorrect since this is used to decrease the latency to access of data
For more information on backups for DynamoDB, please visit the below URL's

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

Ask our Experts

QUESTION 11 UNATTEMPTED

A company has a set of EC2 Instances in a VPC. The IT Security department want to enable monitoring of traffic to just a single Elastic Network Interface for a particular EC2 Instance. How can you achieve this?

- A. Enable VPC Flow logs for the subnet
- B. Enable VPC Flow logs for the ENI ✔
- C. Enable Cloudwatch logs for the ENI
- D. Enable Cloudwatch logs for the subnet

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.
Options C and D are invalid since you need to use VPC Flow logs
Option A is invalid since you can also just enable VPC flow logs on the ENI level
For more information on VPC Flow logs, please visit the below URL's

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

Ask our Experts

QUESTION 12 UNATTEMPTED

A company wants to deploy a set of Instances. The workloads on these instances remain fairly constant in CPU utilization around 40% with brief intervals of peak loads. Which of the following would be the most Cost-effective instance types to be used for the Instances? Select 2 correct answers from the following Options.

- A. T2 Instance type ✔
- B. M4 Instance type
- C. C4 Instance type

☐ **D.** T3 Instance type ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following
Burstable performance instances, which include T3 and T2 instances (https://aws.amazon.com/ec2/instance-types/), are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. Burstable performance instances are well suited for a wide range of general-purpose applications. Examples include microservices, low-latency interactive applications, small and medium databases, virtual desktops, development, build, and stage environments, code repositories, and product prototypes.
Because this is clearly mentioned in the AWS documentation, all other options are invalid
For more information on burstable performance instances, please visit the below URL's

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

Ask our Experts

QUESTION 13 UNATTEMPTED

A company wants to establish a hybrid connection between an On-premise data center and a VPC hosted in AWS. They want to bear the least cost for this connectivity and implement the solution quickly. Which of the following should they consider?

○ **A.** AWS VPC Peering
○ **B.** AWS VPN Managed Connections ✔
○ **C.** AWS Direct Connect
○ **D.** AWS Direct Connect Gateway

Explanation :

Answer – B
The AWS VPN connection is the most cost effective. It might not be the most reliable and you are dependent on the Internet bandwidth, but the question mentions that cost is a factor

Options C and D should only be considered for low latency connections and when you are willing to bear the cost for an AWS Direct Connect connection
Option A is invalid since this is only used to connect VPC's
For more information on AWS Managed VPN Connections, please visit the below URL's

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

Ask our Experts

QUESTION 14 UNATTEMPTED

You work as SysOps Administrator for a company. The company has a set of Instances in a private subnet that need to access the KMS service. Due to security reasons, the traffic cannot cross over to the Internet. Which of the following addition to the Infrastructure would help you achieve this requirement?

- A. NAT Instance
- B. NAT gateway
- C. VPN connection
- D. VPC endpoint ✔

Explanation :

Answer - D
The AWS Documentation mentions the following
You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network.
AWS KMS supports Amazon Virtual Private Cloud (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Introduction.html) (Amazon VPC) interface endpoints (https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html) that are powered by AWS PrivateLink (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Introduction.html#what-is-privatelink). Each VPC endpoint is represented by one or more Elastic Network Interfaces (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html) (ENIs) with private IP addresses in your VPC subnets.

The VPC interface endpoint connects your VPC directly to AWS KMS without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. The instances in your VPC do not need public IP addresses to communicate with AWS KMS.
All other options would cause the traffic to go via the Internet
For more information on Endpoints, please visit the below URL's

- https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html (https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html)

Ask our Experts

QUESTION 15 UNATTEMPTED

You're team has setup a VPC with multiple subnets. There is a web server hosted in one subnet and a database server hosted in another subnet. During initial test, it could be seen that the web server was not able to establish communication with the database server. Which of the following would you need to check for this?

- **A.** Ensure that the Internet gateway is attached to the VPC
- **B.** Ensure that the route tables are modified so that communication is possible across subnets
- **C.** Ensure the security group for the database server is allowing the required inbound communication ✔
- **D.** Ensure a public IP is assigned to the database server

Explanation :

Answer – C
The AWS Documentation mentions the following
A *security group* acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.
Option A is incorrect since this is an internal communication problem
Option D is incorrect since the communication needs to be done via the Private IP
For more information on security groups, please visit the below URL's

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

Note:
Route table defines the traffic goes in and out of the subnet. Not between two subnets. Hence, option B can't be the correct answer.

Ask our Experts

QUESTION 16 UNATTEMPTED

A company has a set of EC2 Instances placed behind a Classic Load Balancer. There is a requirement from the IT Security department to get a list of the client's IP addresses which establish a connection with the Load balancer. Which of the following can help with this requirement?

- A. Use Cloudtrail logs
- B. Use Cloudwatch metrics for the ELB
- C. Enable Access logs for the ELB ✔
- D. Use the AWS Config service

Explanation :

Answer – C
The AWS Documentation mentions the following
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyse traffic patterns and to troubleshoot issues.
Option A is incorrect since this service is used for API monitoring
Option B is incorrect since the metrics will not provide the required data
Option D is incorrect since this a configuration service
For more information on the Classic Load Balancer, please visit the below URL's

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

Ask our Experts

QUESTION 17 UNATTEMPTED

You have a set of EC2 Instances defined in a subnet. The logs from the underlying apache web servers installed on these servers need to be sent over to Cloudwatch. Which of the following needs to be implemented to achieve this? Choose 2 answers from the options given below

- [x] **A.** Install the Cloudwatch agent on the servers ✔
- [ ] **B.** Install the AWS CLI on the servers
- [x] **C.** Ensure an IAM Role with permissions to access Cloudwatch is attached to the server ✔
- [ ] **D.** Ensure an IAM Role with permissions to access Cloudtrail is attached to the server

Explanation :

Answer – A and C
The AWS Documentation mentions the following
The unified CloudWatch agent enables you to do the following:

- Collect more system-level metrics from Amazon EC2 instances, including in-guest metrics, in addition to the metrics listed in Amazon EC2 Metrics and Dimensions (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ec2-metricscollected.html). The additional metrics are listed in Metrics Collected by the CloudWatch Agent (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html).
- Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS.
- Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.

Option B is incorrect we need to use the Cloudwatch agent which is specifically built for the purpose of sending logs from the server
Option D is incorrect since the logs need to be sent to Cloudwatch and not Cloudtrail
For more information on using the Cloudwatch agent, please visit the below URL's

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html)

Ask our Experts

QUESTION 18 UNATTEMPTED

A company wants to setup EC2 Instances in AWS. These instances will be hosting databases which will have a lot of read and write activity. You need to provision the volumes and also ensure that metrics for the volume are available and updated over a 2-minute duration. These instances will be hosting mission-critical transactional databases and they will require consistent baseline performance with low latency.

Which of the following would you implement?

- A. Choose the volume type as General Purpose SSD
- B. Choose the volume type as Provisioned IOPS ✔
- C. Enable Basic Monitoring for the EBS Volume
- D. Enable detailed Monitoring for the EBS Volume

Explanation :

Answer – B

The AWS Documentation mentions the following

Monitoring Volumes with CloudWatch

CloudWatch metrics are statistical data that you can use to view, analyze, and set alarms on the operational behavior of your volumes.

The following table describes the types of monitoring data available for your Amazon EBS volumes.

Type	Description
Basic	Data is available automatically in 5-minute periods at no charge. This includes data for the root device volumes for EBS-backed instances.
Detailed	Provisioned IOPS SSD (io1) volumes automatically send one-minute metrics to CloudWatch.

- Option A is incorrect since Provisioned IOPS is better if you need to host a workload with more read and write activity
- Option C is incorrect since basic monitoring will not fulfil the 2-minute monitoring requirement

- Option D is incorrect because Provisioned IOPS SSD (io1) volumes automatically send one-minute metrics to CloudWatch. We don't need to explicitly enable detailed monitoring for that.

Note:
This is from the docs:
Amazon EBS Metrics
Amazon Elastic Block Store (Amazon EBS) sends data points to CloudWatch for several metrics. Amazon EBS General Purpose SSD (gp2), Throughput Optimized HDD (st1) , Cold HDD (sc1), and Magnetic (standard) volumes automatically send five-minute metrics to CloudWatch. Provisioned IOPS SSD (io1) volumes automatically send one-minute metrics to CloudWatch. Data is only reported to CloudWatch when the volume is attached to an instance.
For more information on monitoring volume status, please visit the below URL's

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-volume-status.html)
- https://aws.amazon.com/ebs/features/ (https://aws.amazon.com/ebs/features/)

Ask our Experts

QUESTION 19 UNATTEMPTED

You work as a SysOps Administrator for a company. They have provisioned a couple of Elastic Beanstalk environments. It needs to be ensured that for all new deployments to the Elastic Beanstalk environment takes the least amount of time. Which of the following would you employ as the deployment mechanism?

- A. All at once ✔
- B. Rolling
- C. Immutable
- D. Blue/green

Explanation :

Answer – A
The AWS Documentation mentions the following

Deployment Methods

Method	Impact of Failed Deployment	Deploy Time	Zero Downtime	No DNS Change	Rollback Process	Code Deployed To
All at once	Downtime	◷	✗	✓	Manual Redeploy	Existing instances
Rolling	Single batch out of service; any successful batches prior to failure running new application version	◷ ◷ †	✓	✓	Manual Redeploy	Existing instances
Rolling with additional batch	Minimal if first batch fails, otherwise, similar to **Rolling**	◷ ◷ ◷ †	✓	✓	Manual Redeploy	New and existing instances
Immutable	Minimal	◷ ◷ ◷ ◷	✓	✓	Terminate New Instances	New instances
Blue/green	Minimal	◷ ◷ ◷ ◷	✓	✗	Swap URL	New instances

Because the AWS Documentation mentions this clearly, all other options are invalid
For more information on deploying apps to Elastic Beanstalk, please visit the below URL's

- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html)

Note:
Blue green deployment takes least amount of time to switch from old version to new version yes, also least amount of time to roll back, but deploying the new version before switching to it, does take longest, because it has to create the complete infrastructure from scratch

You have to launch a new environment with the new version and perform a CNAME swap for a blue/green deployment (https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html).

All at once will take the least amount of time , the reason for that is, all instances get stopped immediately, and updated at the same time

With the other deployment methods, it differ in granularity, where it stop some instances, update them, once they complete and working, it do the next batch of instances.

Refer screenshot for "Deploy Time" column.

QUESTION 20 UNATTEMPTED

A company has a set of programming scripts which are used to perform scheduled tasks. These scripts need to be migrated from their on-premise environment. Which of the following can be used to host the scripts ensuring that cost is optimized?

- A. AWS EC2
- B. AWS Elastic Beanstalk
- C. AWS Opswork
- D. AWS Lambda ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running.
With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.
All other options are not cost-effective options
For more information on AWS Lambda, please visit the below URL's

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

Ask our Experts

QUESTION 21 UNATTEMPTED

A company is setting up an S3 bucket. The users should only have access to read and write objects to the bucket. They should not have permissions to delete objects from the bucket. Which of the following would need to be setup for this purpose?

- A. Enable versioning on the bucket
- B. Attach a bucket policy ✔
- C. Enable MFA Delete on the bucket

○ **D.** Enable CRR for the bucket

Explanation :

Answer – B
An example is given in the AWS Documentation

Amazon S3: Allows Read and Write Access to a Specific S3 Bucket

This example shows how you might create a policy that allows `Read` and `Write` access to a specific S3 bucket. This policy provides the permissions necessary to complete this action using the AWS API or AWS CLI only. To use this policy, replace the red text in the example policy with your own information.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["s3:ListBucket"],
         "Resource": ["arn:aws:s3:::<BUCKET-NAME>"]
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": ["arn:aws:s3:::<BUCKET-NAME>/*"]
      }
   ]
}
```

Options A and C are incorrect since these are used to help from accidental deletion of objects from the bucket

Option D is incorrect since CRR is used for Cross region replication for the bucket objects
For more information on this option, please visit the below URL's

- https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html)

Ask our Experts

QUESTION 22 UNATTEMPTED

Your company has a set of Instances on which you have installed scripts to monitor the memory utilization of the server. You need to be notified whenever the memory breaches a certain threshold. How can you accomplish this? Choose 2 answers from the options given below

- [x] **A.** Setup an alarm based on the metric ✔
- [x] **B.** Setup an SNS topic ✔
- [ ] **C.** Setup an SQS queue
- [ ] **D.** Setup Autoscaling

Explanation :

Answer – A and B
The AWS Documentation mentions the following
Amazon CloudWatch uses Amazon SNS to send email. First, create and subscribe to an SNS topic. When you create a CloudWatch alarm, you can add this SNS topic to send an email notification when the alarm changes state
Option C is incorrect since this is used as a queuing service
Option D is incorrect since this used for scaling purposes
For more information on setting up the alarm with SNS, please visit the below URL's
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/US_SetupSNS.html
(https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/US_SetupSNS.html)

Ask our Experts

QUESTION 23 UNATTEMPTED

You work as a SysOps Administrator for a company. They want to configure Route 53 so that as to ensure that if the application in the primary data centre fails, then the traffic gets rerouted to the secondary. This needs to be done automatically. Which of the following routing policy would you use in Route 53?

- A. Simple
- B. Weighted
- C. Latency
- D. Failover ✔

Explanation :

Answer - D
The AWS Documentation mentions the following
Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records
Because this is clearly mentioned in the documentation , all other options are incorrect
For more information on the routing policy, please visit the below URL's

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

QUESTION 24 UNATTEMPTED

As a Sysops Administrator for a company, you have been requested to ensure that when snapshots of EBS volumes are completed, that automatically the snapshots are copied to another region for disaster recovery purposes. How can you achieve this? Choose 2 answers from the options given below

- A. Make use of the Cloudwatch Events ✔
- B. Ensure Lambda functions are in place to copy the snapshots ✔
- C. Make use of S3 bucket events

☐ **D.** Create an SNS topic

Explanation :

Answer – A and B
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 C is incorrect since this should only be used for S3 bucket events
Option D is incorrect since this is used for notification purposes
For more information on Cloudwatch events, please visit the below URL's

- 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

QUESTION 25 UNATTEMPTED

Your company has a series of Cloudformation templates. There is a requirement to ensure that all API calls to the cloudformation templates are recorded. Which of the following would you use for this purpose?

○ **A.** AWS Config
○ **B.** AWS Cloudwatch
○ **C.** AWS Trusted Advisor
○ **D.** AWS Cloudtrail ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
AWS CloudFormation is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS CloudFormation. CloudTrail captures all API calls for AWS CloudFormation as events, including calls from the AWS CloudFormation console and from code

calls to the AWS CloudFormation APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS CloudFormation. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to AWS CloudFormation, the IP address from which the request was made, who made the request, when it was made, and additional details.
Option A is incorrect since this is a configuration service
Option B is incorrect since this is a monitoring and logging service
Option C is incorrect since this is used as a recommendations service
For more information on Cloudtrail logging, please visit the below URL's

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-api-logging-cloudtrail.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-api-logging-cloudtrail.html)

Ask our Experts

QUESTION 26 UNATTEMPTED

One of the development teams has developed an application that interacts with a DynamoDB table. The application now needs to be hosted on an EC2 Instance. Which of the following would need to be implemented as part of this deployment?

- A. Ensure that the EBS volume used is Provisioned IOPS
- B. Ensure an IAM Role is attached to the EC2 Instance ✔
- C. Ensure that you choose an EBS Optimized Instance
- D. Ensure that you choose a Network Optimized Instance

Explanation :

Answer – B
The AWS Documentation mentions the following
Applications that run on an EC2 instance must include AWS credentials in their AWS API requests. You could have your developers store AWS credentials directly within the EC2 instance and allow applications in that instance to use those credentials. But developers would then have to manage the credentials and ensure that they securely pass the credentials to each instance and update each EC2 instance when it's time to rotate the credentials. That's a lot of additional work.
Instead, you can and should use an IAM role to manage temporary credentials for applications that run on an EC2 instance. When you use a role, you don't have to distribute long-term credentials (such as a user name and password or access keys) to an EC2 instance. Instead, the role supplies temporary

permissions that applications can use when they make calls to other AWS resources. When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.
All other options are incorrect since we can't make any recommendations on the EBS and network recommendations since not much information is provided about the application
For more information on IAM Roles, please visit the below URL's

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

Your company is planning on hosting a web-based application on an EC2 instance. The application will be used by users across the world. Which of the following can be used to speed up the distribution of content to the users?

- A. AWS Cloudfront ✔
- B. AWS SNS
- C. AWS SQS
- D. AWS Lambda

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.
Option B is incorrect since this is a notification service
Option C is incorrect since this is a queue service
Option D is incorrect since this is a compute service
For more information on AWS Cloudfront, please visit the below URL's

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

Ask our Experts

QUESTION 28 UNATTEMPTED

An application is being setup by launching EC2 Instances and an Elastic Load balancer. It needs to be ensured that the application is made highly available and also a uniform distribution of traffic across the various backend nodes. How can you accomplish this? Choose 2 answers from the options given below?

- [ ] **A.** Ensure that the Instances are launched across multiple regions
- [ ] **B.** Ensure that the Instances are launched across multiple availability zones ✔
- [ ] **C.** Ensure that cross zone load balancing is enabled on the load balancer ✔
- [ ] **D.** Ensure that the load balancer is created across multiple regions

Explanation :

Answer – B and C
For maximum availability ensure that the Instances are placed across multiple availability zones
The AWS Documentation mentions the following
When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.
Options A and D are incorrect since the resources need to be created in the same region
For more information on the Network Load Balancer, please visit the below URL's

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

Ask our Experts

QUESTION 29 UNATTEMPTED

You have been tasked with the setup of an application which will consist of EC2 Instances and an Elastic Load Balancer. The EC2 instances need to be able to withstand CPU bursts for long periods of time. Also, the application requests to the

backend servers need to be routed based on the URL paths. Which of the following need to be considered in the implementation plan. Choose 2 answers from the options given below.

- [ ] **A.** Choose the t2 family of instances. Enable t2.unlimited on the instances ✔
- [ ] **B.** Ensure that you create an Application Load Balancer ✔
- [ ] **C.** Ensure that you create a Network Load Balancer
- [ ] **D.** Ensure to choose an EBS optimized instance

Explanation :

Answer – A and B
The AWS Documentation mentions the following
Using an Application Load Balancer instead of a Classic Load Balancer has the following benefits:

· Support for path-based routing. You can configure rules for your listener that forward requests based on the URL in the request. This enables you to structure your application as smaller services, and route requests to the correct service based on the content of the URL.

· Support for host-based routing. You can configure rules for your listener that forward requests based on the host field in the HTTP header. This enables you to route requests to multiple domains using a single load balancer.

Burstable performance instances, which include T3 and T2 instances (https://aws.amazon.com/ec2/instance-types/), are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload. Burstable performance instances are well suited for a wide range of general-purpose applications. Examples include microservices, low-latency interactive applications, small and medium databases, virtual desktops, development, build, and stage environments, code repositories, and product prototypes.
Option C is incorrect since this load balancer does not support path-based routing
Option D is incorrect since there is no mention for optimizing the path to EBS Volumes
For more information on the Application Load Balancer and the t2 instances, please visit the below URL's

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

Ask our Experts

QUESTION 30 UNATTEMPTED

Your team is creating a Cloudformation stack that is going to make use of a template to create a VPC, an Internet gateway and EC2 Instances with public IP address. Which of the following should you consider to avoid running into errors in the template deployment?

- **A.** Ensure that the parameter section is included in the template
- **B.** Ensure that the DependsOn attribute is specified in the template ✔
- **C.** Ensure that the DeletionPolicy is mentioned in specified in the template
- **D.** Ensure that the UpdatePolicy is mentioned in specified in the template

Explanation :

Answer – B
The AWS Documentation mentions the following

When a DependsOn attribute is required

VPC-gateway attachment

Some resources in a VPC require a gateway (either an Internet or VPN gateway). If your AWS CloudFormation template defines a VPC, a gateway, and a gateway attachment, any resources that require the gateway are dependent on the gateway attachment. For example, an Amazon EC2 instance with a public IP address is dependent on the VPC-gateway attachment if the `VPC` and `InternetGateway` resources are also declared in the same template.

Option A is incorrect since this is used to accept dynamic parameters in the template
Option C is incorrect since the DeletionPolicy attribute is used to preserve or backup a resource when its stack is deleted.
Option D is incorrect since the UpdatePolicy attribute is used to specify how AWS CloudFormation handles updates to the AWS::AutoScaling::AutoScalingGroup (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as-group.html) orAWS::Lambda::Alias (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-lambda-alias.html) resource.
For more information on the depends on attribute, please visit the below URL's

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

Ask our Experts

QUESTION 31 UNATTEMPTED

You've just provisioned an AWS RDS Instance. There is a large dataset that is going to be loaded in the database. Which of the following metric would you ideally monitor during the load process? Choose 2 answers from the options given below

- [x] **A.** Disk Queue Depth ✔
- [x] **B.** Free Storage Space ✔
- [ ] **C.** Replica Lag
- [ ] **D.** Read IOPS

Explanation :

Answer – A and B
The AWS Documentation mentions the following
If your DB instance runs out of storage space, it might no longer be available. We highly recommend that you constantly monitor the FreeStorageSpace metric published in CloudWatch to ensure that your DB instance has enough free storage space.
Also, the number of outstanding IOs (read/write requests) waiting to access the disk.
Option C is incorrect since this is used to record the amount of time a Read Replica DB instance lags behind the source DB instance. Applies to MySQL, MariaDB, and PostgreSQL Read Replicas.
Option D is incorrect since this is a write intensive operation for the loading of data
For more information on metrics for RDS, please visit the below URL's

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch)
- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/rds-metricscollected.html)

Ask our Experts

QUESTION 32 UNATTEMPTED

Your company has an existing RDS Instance-MySQL with data already in place. The IT Security department is now mandating that all data be encrypted at rest. Which of the following are options you can take to comply with this requirement? Choose 2 answers from the options given below

- [ ] **A.** Enable encryption for the existing database
- [ ] **B.** Recreate a new DB with the encryption enabled. Copy the existing data to the new DB. ✔
- [ ] **C.** Create a snapshot of the existing DB. Create an encrypted copy of that snapshot ✔
- [ ] **D.** Create a snapshot of the existing EBS Volumes. Create an encrypted copy of that snapshot

Explanation :

Answer – B and C
The AWS Documentation mentions the following
You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created.
However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.
Since this is clearly mentioned in the AWS documentation, all other options are incorrect
For more information on metrics for RDS, please visit the below URL's

- 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 33 UNATTEMPTED

Your company has a large set of resources in AWS. They want to get the utilization of the resources and see places where they could optimize on the costs if possible. Which of the following can be used for this purpose?

- A. AWS Config
- B. AWS Inspector
- C. AWS Cost and Usage reports ✔
- D. AWS Cloudtrail

Explanation :

Answer – C
The AWS Documentation mentions the following
The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account. The report contains line items for each unique combination of AWS product, usage type, and operation that your AWS account uses. You can customize the AWS Cost and Usage report to aggregate the information either by the hour or by the day.
Option A is incorrect since this is just a configuration service
Option B is incorrect since this used to check the server for vulnerabilities
Option D is incorrect since this is used for API monitoring
For more information on cost usage reports, please visit the below URL's

- https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-costusage.html (https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-costusage.html)

Ask our Experts

QUESTION 34 UNATTEMPTED

A development team has developed an application based on Docker containers. They need to host this on AWS. It needs to be setup ensuring that there are no maintenance overheads incurred in the deployment. Which of the following would you use for this purpose?

- A. Amazon ECS ✔
- B. Amazon EC2
- C. Amazon Lambda
- D. Amazon API gateway

Explanation :

Answer – A
The AWS Documentation mentions the following
Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high-performance container (https://aws.amazon.com/containers/) orchestration service that supports Docker (https://aws.amazon.com/docker/) containers and allows you to easily run and scale containerized applications on AWS. Amazon ECS eliminates the need for you to install and operate your own container orchestration software, manage and scale a cluster of virtual machines, or schedule containers on those virtual machines.
Option B is incorrect since here you would need to manage the resources
Options C and D are incorrect since these are not the right services to host Docker container-based applications
For more information on AWS ECS, please visit the below URL's

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

Ask our Experts

QUESTION 35 UNATTEMPTED

You need to establish a backup and archiving strategy for your company using AWS. Documents should be immediately accessible for 3 months and available for 5 years for compliance reasons. Which AWS service fulfills these requirements in the most cost-effective way?

- **A.** Use StorageGateway to store data to S3 and use life-cycle policies to move the data into Redshift for long-time archiving
- **B.** Use DirectConnect to upload data to S3 and use IAM policies to move the data into Glacier for longtime archiving
- **C.** Upload the data on EBS, use life-cycle policies to move EBS snapshots into S3 and later into Glacier for long-time archiving
- **D.** Upload data to S3 and use life-cycle policies to move the data into Glacier for long-time archiving ✔

Explanation :

Answer – D

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

· Transition actions—Define when objects transition to another storage class (https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html). For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.

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

Options A and C are incorrect since lifecycle policies are used for S3
Option B is incorrect since IAM policies are not used for movement of data
For more information on S3 object lifecycle, please visit the below URL's

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

Ask our Experts

QUESTION 36 UNATTEMPTED

An application server running on an Amazon EC2 instance in a private subnet in a VPC must connect to the internet to download software updates.

How can this be achieved?

- **A.** Create a NAT gateway and update the route table. ✔
- **B.** Assign an Elastic IP address to the EC2 instance.
- **C.** Update the security group for the EC2 instance to allow Port 80 from 0.0.0.0/0
- **D.** Update the rule for the inbound network access control list for the subnet containing the EC2 instance.

Explanation :

Answer – A
The AWS Documentation mentions the following

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
All other options are implementation schemes for allowing access to the Internet via a public subnet.
And here we have a private subnet.
For more information on the NAT gateway, please visit the below URL's

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

Ask our Experts

QUESTION 37 UNATTEMPTED

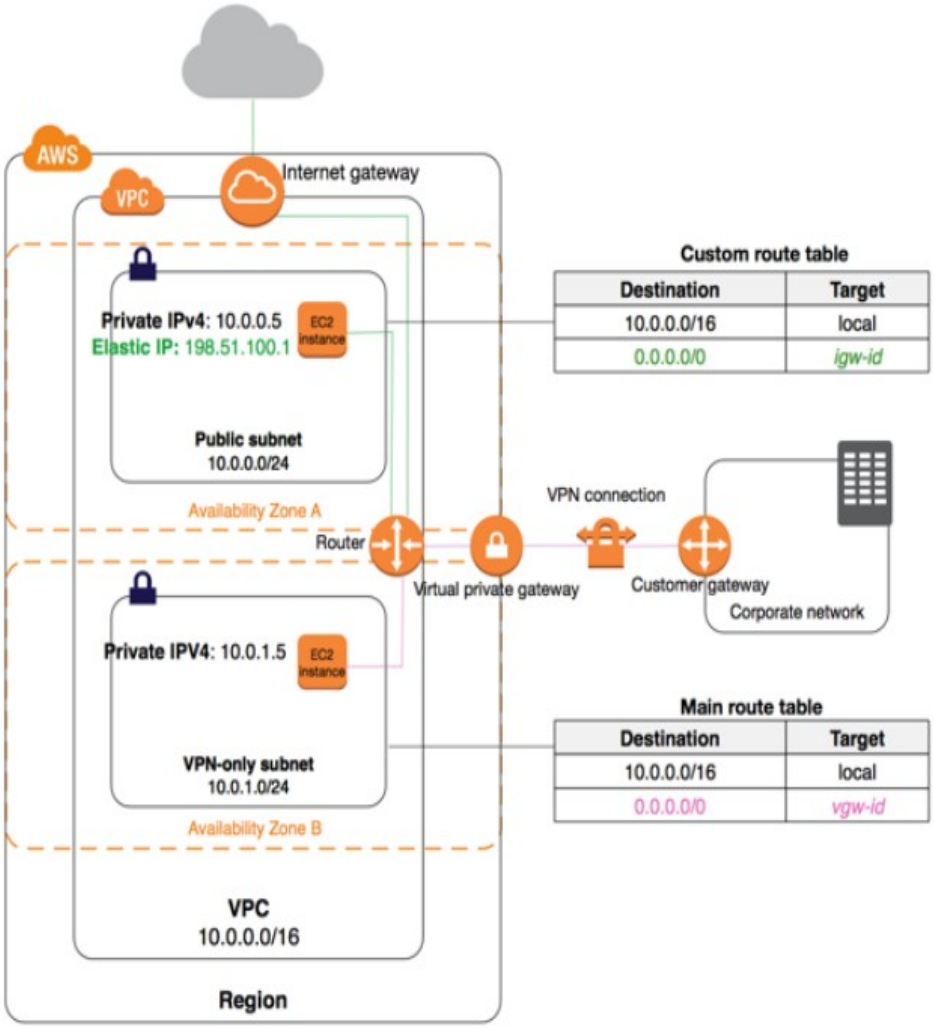
An organization is trying to establish a static VPN connection between an on-premises network and an Amazon VPC. A SysOps Administrator has created the virtual private gateway., VPN connection, and the customer gateway. The customer side of the router is also configured and the connection status shows UP in the console. However, when the Administrator attempts to connect an Amazon EC2 instance in the Amazon VPC from one of the on-premises virtual machines, it does not work.

How should the route table in the Amazon VPC subnet be modified to remediate the issue?

- **A.** Add the route for the virtual private gateway ✔
- **B.** Add the route for the VPC endpoint
- **C.** Add the route to the internet gateway
- **D.** Add the route for the customer gateway

Explanation :

Answer – A
The below diagram from the AWS Documentation shows that the route needs to be added for the Virtual private gateway



All other options are incorrect since the main reason is that the virtual private gateway is not assigned to the Route table

For more information on Route Tables, please visit the below URL's
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html
(https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html)

Ask our Experts

QUESTION 38 UNATTEMPTED

A company monitors its AWS environment with Amazon CloudWatch and has configured several CloudWatch alarms. When an alarm is triggered, both the Developer and the Product Manager must be notified immediately

Which service is recommended to deliver the notice?

- A. Amazon Simple Email Service
- B. Amazon Simple Queue Service
- C. Amazon Simple Notification Service ✔
- D. Amazon MQ

Explanation :

Answer – C
The AWS Documentation mentions the following
Amazon Simple Notification Service (SNS) is a flexible, fully managed pub/sub messaging (https://aws.amazon.com/pub-sub-messaging/) and mobile notifications service for coordinating the delivery of messages to subscribing endpoints and clients. With SNS you can fan-out messages to a large number of subscribers, including distributed systems and services, and mobile devices. It is easy to set up, operate, and reliably send notifications to all your endpoints – at any scale
Option A is incorrect since this is just an email service and not a notification service
Options B and D are incorrect since these are queue-based services
For more information on the AWS SNS service, please visit the below URL's

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

Ask our Experts

QUESTION 39 UNATTEMPTED

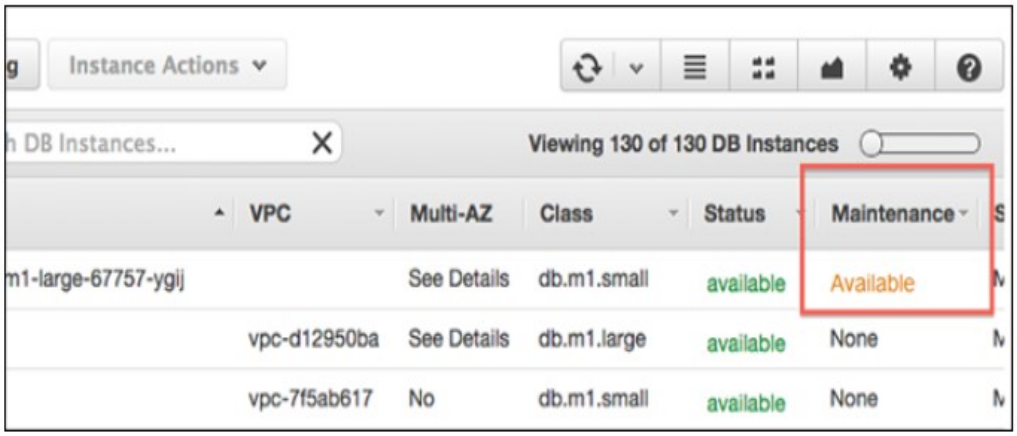
A SysOps Administrator is auditing the OS patching process of Amazon RDS instances as a part of an organization's internal annual review process.

Which AWS service can the Administrator use to report on the RDS?

- A. AWS Artifact
- B. Amazon RDS console ✔
- C. Amazon Inspector
- D. AWS Trusted Advisor

Explanation :

Answer – B
This can be viewed via the dashboard



Since this is clearly available from the dashboard, all other options are incorrect

For more information on maintaining a database, please visit the below URL's

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.htm (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html)

Ask our Experts

QUESTION 40 UNATTEMPTED

A SysOps Administrator is tasked with making the AWS Management Console and AWS CLI access more streamlined and secure. The company uses Active Directory for internal IT resources, but for AWS, users share the account owner (root) login.

What is the recommended way for the Administrator to make access more secure and streamlined?

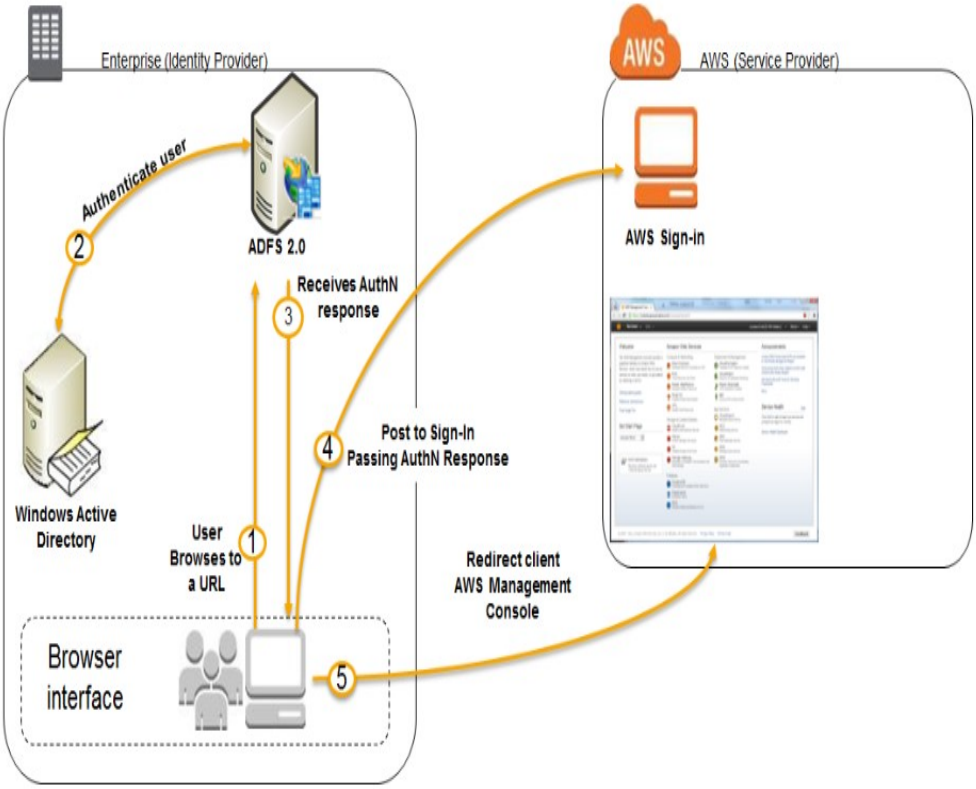
- **A.** Store Active Directory logins using reversible encryption. Implement a script to query the Active Directory logins for Administrators and synchronize passwords with the matching AWS logins.
- **B.** Create IAM users for each user that requires AWS access and mirror their groups in Active Directory with AWS IAM Groups. Allow users to keep passwords synchronized if they prefer.
- **C.** Configure a SAML federation between AWS and the corporate Active Directory. Map Active Directory groups to IAM groups to manage user permissions ✔
- **D.** Move users to SSH keys and discontinue use of the root login. Make sure that keys are rotated every 90 days and disable password authentication to the console.

Explanation :

Answer – C
The preferred setup is given in the AWS Documentation

How Integration Between AD FS and AWS Works

Before we get too far into the configuration details, let's walk through how this all works.



Since the preferred setup is already given, all other options are incorrect

For more information on the preferred setup, please visit the below URL's

- https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/ (https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/)

Ask our Experts

QUESTION 41 UNATTEMPTED

An application running on Amazon EC2 processes files that are stored in an Amazon S3 bucket. What is the BEST way to provide the application with access to the S3 bucket?

- **A.** Create a new account with permissions to the S3 bucket. Provide the application Developer with the access key ID and secret access key to embedded into the application.
- **B.** Create a new access key for the root user. Provide the Developer with the access key ID and secret access key embedded into the application
- **C.** Set the bucket properties in "Static website hosting" to "use this bucket to host a website", and give the Developer the website URL.
- **D.** Create an IAM role that has access to the S3 bucket. Attach the role to the EC2 instance running the application. ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
Applications that run on an EC2 instance must include AWS credentials in their AWS API requests. You could have your developers store AWS credentials directly within the EC2 instance and allow applications in that instance to use those credentials. But developers would then have to manage the credentials and ensure that they securely pass the credentials to each instance and update each EC2 instance when it's time to rotate the credentials. That's a lot of additional work.
Instead, you can and should use an IAM role to manage temporary credentials for applications that run on an EC2 instance. When you use a role, you don't have to distribute long-term credentials (such as a user name and password or access keys) to an EC2 instance. Instead, the role supplies temporary permissions that applications can use when they make calls to other AWS resources. When you launch an EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.
Options A and B are incorrect since using Access keys is not a secure way to allowing access to other resources
Option C is incorrect since this should only be used for hosting a static web site
For more information on IAM Roles, please visit the below URL's

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html)

Ask our Experts

QUESTION 42 UNATTEMPTED

A SysOps Administrator has been notified of an issue involving an Auto Scaling group with hundreds of instances. When the launch configuration is updated, the process for the Auto Scaling group is taking multiple nodes offline at the same time, which is impacting customers. The Application team is using AWS CloudFormation to update the application by changing a parameter to the version of code it wants to enable.

What can the Administrator do to limit the impact on customers while the update is being performed?

- **A.** Edit the user data script to add a description of the instances in the Auto Scaling group, and run AWS EC2 terminate-instances against the next oldest instance id.
- **B.** Add the Update Policy attribute in Cloud Formation, and also enable the WaitOnResourceSignals property. Append a health check at the end of the user data script to signal CloudFormation that it was successful. ✔
- **C.** Convert the Auto Scaling group to many individual instances. Have the application team update one machine at a time in Cloud Formation.
- **D.** Add a DependsOn attribute to the Auto Scaling group resource in Cloud Formation to depend on the Launch Configuration. Append to the user data script to signal the wait condition.

Explanation :

Answer – B
The AWS Documentation mentions the following
To specify how AWS CloudFormation handles replacement updates for an Auto Scaling group, use the AutoScalingReplacingUpdate policy. This policy enables you to specify whether AWS CloudFormation replaces an Auto Scaling group with a new one or replaces only the instances in the Auto Scaling group.

- Options A and C is incorrect since this will still not prevent the changes of Cloudformation
- Option D is incorrect since the Autoscaling already depends on the Launch Configuration

- For more information on the update policy attribute, please visit the below URL's
- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-updatepolicy.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-updatepolicy.html)

Ask our Experts

QUESTION 43 UNATTEMPTED

Due to recent security incidents, a company has asked a SysOps Administrator to ensure that all AWS CloudFormation stacks that are launched use the latest Windows AMI.

Which strategy will meet this requirement while minimizing management overhead? Please select 2 correct options.

- [ ] **A.** Add a map of the latest AMIs for each region to each template. Use the Fn::FindInMap to launch the correct windows AMI. When new AMI's are released, update the map in each template.
- [ ] **B.** Use the Parameters section in the template to specify the Systems Manager (SSM) Parameter, which contains the latest version of Windows regional AMI ID. ✔
- [ ] **C.** Use an API call to get the available Windows AMIs and sort them by the lowest ImageID, update the template if the Image ID changes.
- [ ] **D.** Subscribe to Windows AMI notifications using Amazon SNS and trigger an AWS Lambda function that updates the template when a new AMI is released. ✔

Explanation :

Answer: B and D

Consider the use case of updating Amazon Machine Image (AMI) IDs for the EC2 instances in your Cloud Formation templates. Normally, you might map AMI IDs to specific instance types and Regions. Then to update these, you would manually change them in each of your templates. Or you would be using a custom resource with an AWS Lambda function that gets the IDs of the latest AMIs for the Region and instance type that you're using. Arguably, neither of these methods is very convenient. You can use the public parameter variable for the Windows AMI ID in your template. You don't need to worry about how to fetch the latest AMI IDs. This SSM parameter will be updated whenever there is a newer version available. Whenever you decide to update the EC2 instances in your Cloud Formation template to use the new AMI ID, you just call update-stack API on the stack. It will automatically fetch the latest value from the Parameter Store. Also, note that for hierarchical parameters, you need to provide the full path of the parameter name.

- https://aws.amazon.com/blogs/mt/integrating-aws-cloudformation-with-aws-systems-manager-parameter-store/ (https://aws.amazon.com/blogs/mt/integrating-aws-cloudformation-with-aws-systems-manager-parameter-store/)

Ask our Experts

QUESTION 44 UNATTEMPTED

After implementing a multi-region AWS deployment for all production infrastructure, what Amazon Route 53 feature would minimize response time for users?

- A. Hosted zones for specific regions
- B. Health checks with DNS failover
- C. Geolocation routing
- D. Latency –based routing ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.
To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or apex.example.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region. Route 53 responds with the value from the selected record, such as the IP address for a web server.
Because this is mentioned in the documentation, all other options are invalid
For more information on the routing policies, please visit the below URL's

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

QUESTION 45 UNATTEMPTED

A SysOps Administrator is managing an application where Amazon EC2 instances in an Auto Scaling group read messages from an Amazon SQS queue. When the message traffic increases, the EC2 instances fall behind and it takes too long to process the messages.

How can the administrator configure the application to reduce the latency during traffic spikes?

- **A.** Configure the Auto Scaling group to scale based on a schedule.
- **B.** Trigger scaling events based on the number of messages in the queue. ✔
- **C.** Trigger scaling events based on the disk space used on the EC2 instances.
- **D.** Manually increment the Auto Scaling group's desired capacity during traffic spikes

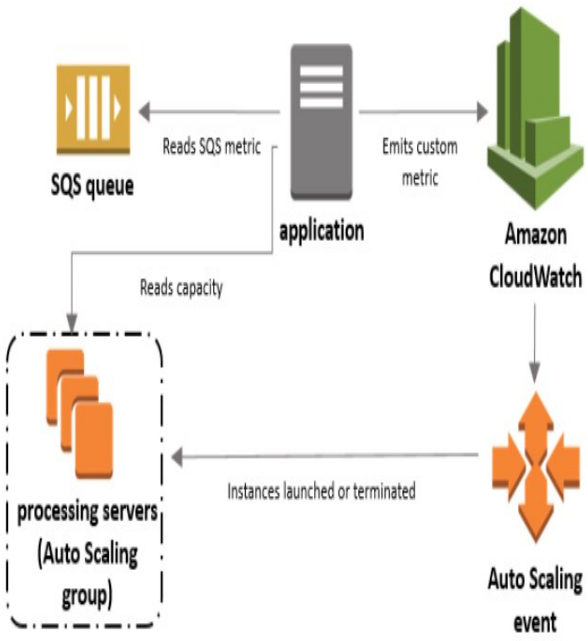
Explanation :

Answer – B
This example is also given in the AWS Documentation

There are three main parts to this configuration:

- An Auto Scaling group to manage EC2 instances for the purposes of processing messages from an SQS queue.
- A custom metric to send to Amazon CloudWatch that measures the number of messages in the queue per EC2 instance in the Auto Scaling group.
- A target tracking policy that configures your Auto Scaling group to scale based on the custom metric and a set target value. CloudWatch alarms invoke the scaling policy.

The following diagram illustrates the architecture of this configuration.



Since the number of messages is the main component for scaling , that should be used in this case.

For more information on scaling based on SQS, please visit the below URL's

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html)

Ask our Experts

QUESTION 46 UNATTEMPTED

An organization recently expanded its AWS infrastructure for its public website into two regions, US East (Ohio) to Asia Pacific (Mumbai), to better serve growing demand in Asia.

What should the SysOps Administrator implement to ensure that users are consistently directed to the best -performing region?

- **A.** Configure AWS WAF to redirect users from Asia to the website using a third-party geolocation service.
- **B.** Use Amazon Route 53 geoproximity routing to direct users in Asia to the website.
- **C.** Configure the existing webserver's Application Load Balancer to redirect distant users to the closer website.
- **D.** Migrate to a Route 53 latency record for the website. ✔

Explanation :

Answer – D
########
The AWS Documentation mentions the following
If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.
To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or apex.example.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region.
Route 53 responds with the value from the selected record, such as the IP address for a web server.
########
Because this is mentioned in the documentation, all other options are invalid
For more information on the routing policies, please visit the below URL's

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

QUESTION 47 UNATTEMPTED

A SysOps Administrator has an Amazon EC2 instance using iPv6.

Which VPC feature allows the instance to communicate with the internet but prevents inbound traffic?

- A. NAT Gateway
- B. NAT instances
- C. Egress –only internet gateway ✔
- D. Internet gateway

Explanation :

Answer - C
The AWS Documentation mentions the following
An egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in your VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with your instances.
Because this is mentioned in the documentation, all other options are invalid
For more information on the egress only gateway, please visit the below URL's

- https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html (https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html)

Ask our Experts

QUESTION 48 UNATTEMPTED

During at security audit, a known vulnerability was discovered in the guest OS of the organization's large Amazon EC2 fleet. A SysOps Administrator must ensure that this vulnerability is mitigated in a timely manner.

What is the MOST efficient way for the Administrator to accomplish this task?

- **A.** Open a case with AWS Support requesting that the deployment of the security patch be prioritized.
- **B.** Deploy the security patch by using AWS Systems Manager for the entire fleet of EC2 instances. ✔
- **C.** Perform a Stop and Start of the EC2 instances to force them to an already-patched state.
- **D.** Have AWS automatically install the security patch during the weekly maintance window.

Explanation :

Answer – B
The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Amazon Linux, and Amazon Linux 2. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Options A and D are incorrect since patching of the servers is the responsibility of the customer
Option C is incorrect the start and stop action will not cause automatic patching
For more information on the Systems Patch Manager, please visit the below URL's

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

Ask our Experts

QUESTION 49 UNATTEMPTED

A company is migrating an application to its AWS environment. The implementation requires the company to deploy up to 40m4.4xlarge instances

What should a SysOps Administrator do prior to launching the instances?

- **A.** Increase service limits from AWS Trusted Advisor before launching new instances.

- **B.** Submit a service limit increase to AWS support specifying the instance type and region ✔
- **C.** Reserve 40 Elastic IP addresses before initiating a request to launch the instances
- **D.** Update the instance count in the AWS Service Catalog default service limits

Explanation :

Answer – B
There is clear limit on the number of instances that can be launched in a region, hence you need to request for a limit increase

Amazon EC2 provides different *resources* that you can use. These resources include images, instances, volumes, and snapshots. When you create your AWS account, we set default limits on these resources on a per-region basis. For example, there is a limit on the number of instances that you can launch in a region. Therefore, when you launch an instance in the US West (Oregon) region, the request must not cause your usage to exceed your current instance limit in that region.

Because this is mentioned in the documentation, all other options are invalid
For more information on the limit increase, please visit the below URL's

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

Ask our Experts

QUESTION 50 UNATTEMPTED

A Systems Administrator is writing a configuration script that requires the public IP of an Amazon EC2 instance on which it is executed

How can the System Administrator obtain the IP address?

- A. From the operating system of the EC2 instance
- B. From the instance metadata ✔
- C. From the user data
- D. From the AMI that was used to launch the EC2 instance

Explanation :

Answer – B
You can get the information from the Instance metadata

This example gets the top-level metadata items. For more information, see Instance Metadata Categories.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

This is the best way for automation and for getting it via the script.

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

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

Ask our Experts

QUESTION 51 UNATTEMPTED

A development team is moving a Ruby-based web application to AWS. The Ruby application basically collect reports from other 3rd party APIs which might sometime take about 15 minutes to respond with some of the reports. After collecting the reports the Ruby application generates intelligent insights. Once operational, the application must be simple to scale, require no environment maintenance, and be easy to update with new versions of the application.

Which AWS service will meet these requirements?

- A. AWS Elastic Beanstalk ✔
- B. AWS CodePipeline
- C. Amazon EC2
- D. AWS Lambda

Explanation :

Answer – A
The AWS Documentation mentions the following
With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.
Option B is incorrect since this service is used for continuous delivery of applications.
Option C is incorrect since here you would need to maintain the environment.
Option D is not the right fit. Even though Lambda supports Ruby, the use case mentions 3rd party APIs which may take a long time to respond. Note that AWS Lambda functions can run only up to 15 minutes per execution.
For more information on AWS Elastic Beanstalk, please visit the below URL's

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

Ask our Experts

QUESTION 52 UNATTEMPTED

A web application is running on AWS. The site runs stateless web servers on three Amazon EC2 instances behind a Classic Load Balancer. The company is receiving complaints from some users about the application performance. Amazon CloudWatch shows that one of the EC2 instances is running at approximately 90% CPU utilization, while the other two are running at approximately 20% CPU utilization.

How can a SysOps Administrator prevent this issue from recurring?

- **A.** Manually provision a fourth EC2 instance and add it to the Classic Load Balancer
- **B.** Review the performance of the database server that supports the web application, then choose a more appropriate instance size and apply the change.
- **C.** Disable sticky sessions on the Classic Load Balancer and check CloudWatch to confirm that the issue has been resolved. ✔
- **D.** Review the number of sessions from the Classic Load Balancer to each web server. Restart any web server that has a significantly more sessions to even out the load.

Explanation :

Answer – C
Here the issue is clearly to do with sticky sessions. Because of this, all sessions are being directed to one server.
The AWS Documentation mentions the following
By default, a Classic Load Balancer routes each request independently to the registered instance with the smallest load. However, you can use the *sticky session* feature (also known as *session affinity*), which enables the load balancer to bind a user's session to a specific instance. This ensures that all requests from the user during the session are sent to the same instance.
Since this is clearly a case of sticky sessions, all other options are invalid
For more information on sticky sessions, please visit the below URL's

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

Ask our Experts

QUESTION 53 UNATTEMPTED

An organization has implemented a file gateway to keep copies of users' home drives in Amazon S3. While conducting an analysis, a SysOps Administrator noticed that files are rarely accessed after 45 days.

What is the most cost-effective way for the Administrator to reduce storage cost while continuing to provide access to the files for the users within 1 to 5 minutes if needed?

- **A.** Enable versioning on the S3 bucket to ensure that all copies of the files are saved
- **B.** Create a lifecycle policy to move files older than 45 days to infrequent Access storage class.
- **C.** Create a lifecycle policy to move files older than 45 days to Amazon Glacier storage class. ✔
- **D.** Create a bucket policy to limit user access to only newer files (those created in less than 45 days)

Explanation :

Answer – C
With new options, Amazon Glacier data can be retrieved in minutes. You can use **Expedited retrievals** to access data in **1 – 5 minutes**.

Please refer this:

- https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/ (https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/)

The AWS Documentation mentions the following
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A *lifecycle configuration* is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:
· Transition actions—Define when objects transition to another storage class (https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html). For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.

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

Option A is incorrect since versioning is used to ensure objects are not accidental deleted
Option B is incorrect since Glacier is much cheaper storage option to migrate older files to
Option D is incorrect since the bucket policy is used for permission access
For more information on S3 object lifecycle, please visit the below URL's

- https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html)
- https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/ (https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/)

Ask our Experts

QUESTION 54 UNATTEMPTED

A company is migrating its applications and data from on-premises to the AWS Cloud, including 500 TB of data that must move to Amazon S3. There are concerns about time, cost and performance. What is the fastest and MOST cost-effective way to perform the migration?

- **A.** Perform a network- based copy of the data from the on-premises network to the destination S3 bucket.
- **B.** Use Direct Connect for copying data from on premise network to destination S3 bucket
- **C.** Use multiple instances of the Snowball client on multiple workstations with multiple Snowball appliance ✔
- **D.** Use AWS Storage Gateway (file gateway type) and facilitate an on-premises copy using the file gateway mount point.

Explanation :

Answer – C
The AWS Documentation mentions the following
AWS Snowball is a service that accelerates transferring large amounts of data into and out of AWS using physical storage devices, bypassing the Internet. Each AWS Snowball device type can transport data at faster-than internet speeds. This transport is done by shipping the data in the devices through a regional carrier. The devices are rugged shipping containers, complete with E Ink shipping labels.
With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premises data centers and Amazon Simple Storage Service (Amazon S3). AWS Snowball uses Snowball appliances and provides powerful interfaces that you can use to create jobs, transfer data, and track the status of your jobs through to completion. By shipping your data in Snowballs, you can transfer large amounts of data at a significantly faster rate than if you were transferring that data over the Internet, saving you time and money.
All other options are incorrect since the best means of transport of data is to use the AWS Snowball device
For more information on AWS Snowball, please visit the below URL's

- https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html (https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html)

Ask our Experts

QUESTION 55 UNATTEMPTED

An application runs on Amazon EC2 instances behind an ELB classic Load Balancer. The instances run in an Auto scaling group access multiple availability zones. Responding to performance complaints, a SysOps Administrator found that instances failing ELB health checks are not being replaced.

What actions should be taken to correct this issue?

- **A.** Configure the Auto scaling group to determine health status using ELB health checks. ✔
- **B.** Delete the auto scaling group and re-create a new one using the same configuration
- **C.** Ensure that UDP port 655 is open on the security group attached to these instances.
- **D.** Terminate these instances and re-launch them as instances within the T2 family.

Explanation :

Answer – A
The AWS Documentation mentions the following
If you configure an Auto Scaling group to determine health status using EC2 status checks only (the default), the instance is unhealthy if it fails the EC2 status checks. However, if you have attached one or more load balancers or target groups to the Auto Scaling group and a load balancer reports that an instance is unhealthy, the instance is not considered unhealthy. Therefore, the instance is not replaced.
If you configure your Auto Scaling group to determine health status using both EC2 status checks and Elastic Load Balancing health checks, it considers the instance unhealthy if it fails either the status checks or the health check. If you attach multiple load balancers to an Auto Scaling group, all of them

must report that the instance is healthy in order for it to consider the instance healthy. If one load balancer reports an instance as unhealthy, the Auto Scaling group replaces the instance, even if other load balancers report it as healthy.
Since this particular case is clearly marked in the AWS documentation, all other options are invalid
For more information on ELB health checks for the Autoscaling Group, please visit the below URL's

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html (https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-elb-healthcheck.html)

Ask our Experts

QUESTION 56 UNATTEMPTED

A team in your company has setup a bucket of web pages in S3. They need web pages in another domain to access the web pages in the S3 bucket. Which of the following would need to be implemented for the bucket?

- A. S3 bucket versioning
- B. S3 MFA Delete
- C. S3 CORS ✔
- D. S3 CRR

Explanation :

Answer – C
The AWS Documentation mentions the following
Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.
Options A and B are incorrect since these options are used to prevent accidental deletion of objects in the bucket
Option D is incorrect since this is used to replicate objects to another region
For more information on CORS, please visit the below URL's

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

Ask our Experts

QUESTION 57 UNATTEMPTED

A team is planning to deploy stacks of application environments using the Opswork service. You need to monitor the logs for the application hosted in the environment. Which of the following service can help achieve this?

- A. AWS Cloudtrail
- B. AWS Cloudwatch Logs ✔
- C. AWS Config
- D. AWS Opsworks logs

Explanation :

Answer – B
The AWS Documentation mentions the following
You can monitor your stacks in the following ways.

- AWS OpsWorks Stacks uses Amazon CloudWatch to provide thirteen custom metrics with detailed monitoring for each instance in the stack.
- AWS OpsWorks Stacks integrates with AWS CloudTrail to log every AWS OpsWorks Stacks API call and store the data in an Amazon S3 bucket.
- You can use Amazon CloudWatch Logs to monitor your stack's system, application, and custom logs.

Option A is incorrect since this is an API monitoring service
Option C is incorrect since this is a configuration service
Option D is incorrect since Opsworks does not have the log service
For more information on monitoring in Opswork, please visit the below URL's

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

Ask our Experts

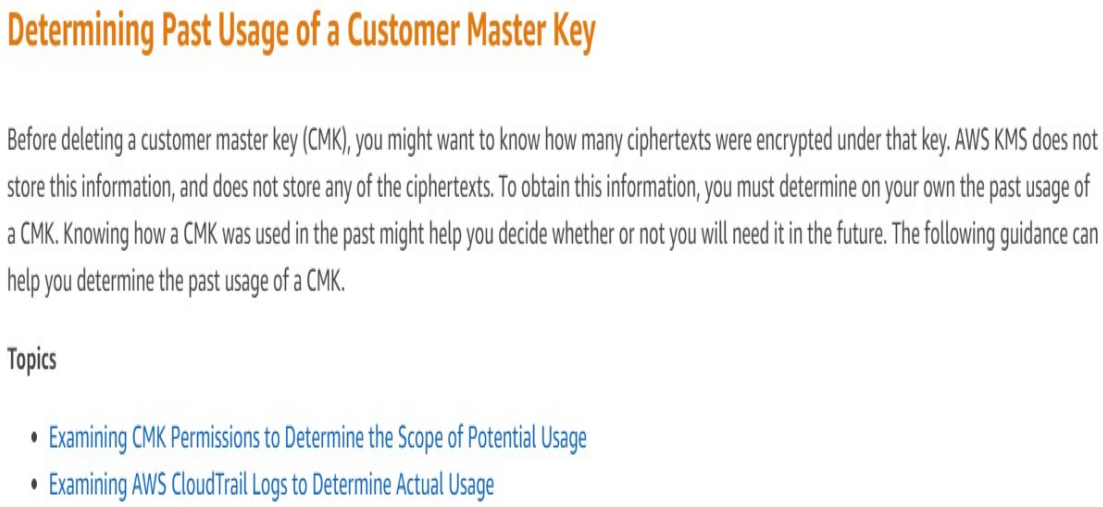
QUESTION 58 UNATTEMPTED

Your company is planning on deleting customer master keys as part of house keeping activities. You need to delete the keys. As a Sysops administrator which of the following would you do to ensure safe deletion of the customer master keys? Choose 2 answers from the options given below

- [ ] **A.** Enable automatic key rotation of the keys
- [ ] **B.** See the CMK permissions to see the usage of the keys ✔
- [ ] **C.** Examine Cloudtrail logs ✔
- [ ] **D.** Examine KMS logs

Explanation :

Answer – B and C
The AWS Documentation mentions the following



Determining Past Usage of a Customer Master Key

Before deleting a customer master key (CMK), you might want to know how many ciphertexts were encrypted under that key. AWS KMS does not store this information, and does not store any of the ciphertexts. To obtain this information, you must determine on your own the past usage of a CMK. Knowing how a CMK was used in the past might help you decide whether or not you will need it in the future. The following guidance can help you determine the past usage of a CMK.

Topics

- Examining CMK Permissions to Determine the Scope of Potential Usage
- Examining AWS CloudTrail Logs to Determine Actual Usage

Option A is incorrect since this is not used prior to deletion of keys

Option D is incorrect since the KMS service does not maintain any logs
For more information on determining the past usage of the Master Key, please visit the below URL's

- https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html (https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-determining-usage.html)

Ask our Experts

QUESTION 59 UNATTEMPTED

You're a SysOps Administrator for a company. You need to be notified of any events that occur in the AWS Personal Health Dashboard. Which of the following can be used for the notification process? Choose 3 answers from the options given below

- [x] **A.** AWS Lambda ✔
- [x] **B.** AWS EC2
- [x] **C.** AWS SQS ✔
- [x] **D.** AWS SNS ✔

Explanation :

Answer – A,C and D
Option B is invalid since this is not available as an event destination
The AWS Documentation mentions the following
You can use Amazon CloudWatch Events to detect and react to changes in the status of AWS Personal Health Dashboard (AWS Health) events. Then, based on the rules that you create, CloudWatch Events invokes one or more target actions when an event matches the values that you specify in a rule. Depending on the type of event, you can send notifications, capture event information, take corrective action, initiate events, or take other actions. You can select the following types of targets when using CloudWatch Events as a part of your AWS Health workflow:

- AWS Lambda functions
- Kinesis streams
- Amazon SQS queues
- Built-in targets (CloudWatch alarm actions)
- Amazon SNS topics

For more information on Cloudwatch events for the Personal Health Dashboard, please visit the below URL's

- https://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html (https://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html)

Ask our Experts

QUESTION 60 UNATTEMPTED

A company is planning on setting up a Redshift cluster in AWS. There is a requirement to ensure logs for the cluster are in place for auditing purposes. Which of the following logs would be available to you? Choose 3 answers from the options given below

- [x] **A.** Connection Logs ✔
- [x] **B.** Transaction Logs
- [x] **C.** User Logs ✔
- [x] **D.** User Activity Logs ✔

Explanation :

Answer – A, C and D
The AWS Documentation mentions the following
Amazon Redshift logs information in the following log files:

- Connection log — logs authentication attempts, and connections and disconnections.
- User log — logs information about changes to database user definitions.
- User activity log — logs each query before it is run on the database.

Option B is invalid since transaction logs are not available
For more information on database auditing, please visit the below URL's

- https://docs.aws.amazon.com/redshift/latest/mgmt/db-auditing.html (https://docs.aws.amazon.com/redshift/latest/mgmt/db-auditing.html)

Ask our Experts

QUESTION 61 UNATTEMPTED

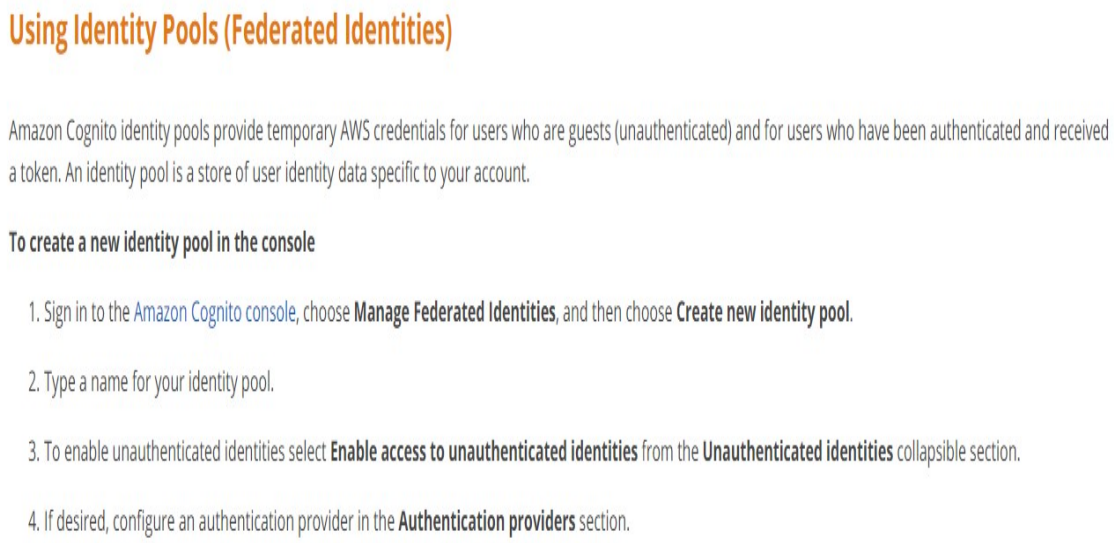
A team in your company wants to develop a mobile based application that would make use of AWS resources. The users should have the ability to log in with existing credentials such as Facebook, but there also be the ability for guest user access as well. Which of the following would be the ideal implementation for this?

- **A.** Create an IAM user with public access

- B. Create an IAM group with public access
- C. Use AWS Cognito with unauthenticated access enabled ✔
- D. Use AWS STS with SAML

Explanation :

Answer – C
This is also mentioned in the AWS Documentation



Using Identity Pools (Federated Identities)

Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.

To create a new identity pool in the console

1. Sign in to the Amazon Cognito console, choose **Manage Federated Identities**, and then choose **Create new identity pool**.
2. Type a name for your identity pool.
3. To enable unauthenticated identities select **Enable access to unauthenticated identities** from the **Unauthenticated identities** collapsible section.
4. If desired, configure an authentication provider in the **Authentication providers** section.

Options A and B are incorrect since it's not the right approach to use IAM users or groups for access for mobile based applications

Option D is incorrect since SAML is used for federated access.
For more information on identity pools , please refer to the below URL

- https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html (https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html)

Ask our Experts

QUESTION 62 UNATTEMPTED

A company has been using the AWS RDS-MySQL Instance. There is a requirement now to disable backups for the AWS RDS Instance. You are trying to set the retention period to 0 to disable backups, but this is resulting in an error. Which of the following could be the possible reason for the error?

- A. There are already backups in place
- B. There is a Read replica in place ✔
- C. You cannot disable backups
- D. The database should be taken offline to disable backups

Explanation :

Answer - B
The AWS Documentation mentions the following
There are several reasons why you may need to set the backup retention period to 0. For example, you can disable automatic backups immediately by setting the retention period to 0. If you set the value to 0 and receive a message saying that the retention period must be between 1 and 35, check to make sure you haven't setup a read replica for the instance. Read replicas require backups for managing read replica logs, thus, you can't set the retention period of 0.
Since this is clearly mentioned in the AWS documentation, all other options are invalid
For more information on Troubleshooting AWS RDS , please refer to the below URL

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

Ask our Experts

QUESTION 63 UNATTEMPTED

A team of developers in a company are planning on using the AWS Kinesis service. The IT Security department has mandated at all data be secured at rest. As a SysOps Administrator, how can you ensure this in the best way possible?

- A. Use the SDK for Kinesis to encrypt the data before being stored at rest
- B. Enable server-side encryption for Kinesis streams ✔
- C. Enable client-side encryption for Kinesis streams

D. Use the AWS CLI to encrypt the data

Explanation :

Answer – B
The easiest way is to use the in-built server-side encryption that is available with Kinesis streams
The AWS Documentation mentions the following
Server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an AWS KMS customer master key (CMK) you specify. Data is encrypted before it's written to the Kinesis stream storage layer, and decrypted after it's retrieved from storage. As a result, your data is encrypted at rest within the Kinesis Data Streams service. This allows you to meet strict regulatory requirements and enhance the security of your data.
Options A and C are invalid since this would involve too much of effort for encrypting and decrypting to the streams
Option D is invalid since this is the same as encrypting the data before it reaches the stream
For more information on server-side encryption with streams , please refer to the below URL

- https://docs.aws.amazon.com/streams/latest/dev/what-is-sse.html (https://docs.aws.amazon.com/streams/latest/dev/what-is-sse.html)

Ask our Experts

QUESTION 64 UNATTEMPTED

Your company is developing a solution that will make use of DynamoDB tables. Due to the nature of the application, the data is needed across a couple of regions across the world. As the Sysops administrator for the company , which of the following would you implement reduce the latency of requests to DynamoDB from different regions?

A. Enable Multi-AZ for the DynamoDB table
B. Enable global tables for DynamoDB ✔
C. Enable Indexes for the table
D. Increase the read and write throughput for the table

Explanation :

Answer - B

The AWS Documentation mentions the following
Amazon DynamoDB global tables provide a fully managed solution for deploying a multi-region, multi-master database, without having to build and maintain your own replication solution. When you create a global table, you specify the AWS regions where you want the table to be available. DynamoDB performs all of the necessary tasks to create identical tables in these regions and propagate ongoing data changes to all of them.
For more information on Global tables , please refer to the below URL

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

Ask our Experts

QUESTION 65 UNATTEMPTED

A company is storing sensitive data in their S3 bucket. The company policy states that all objects in the S3 bucket need to be encrypted at rest. As a Sysops administrator, you need to ensure that the right permissions are set on the bucket. Which of the following would you implement for this requirement?

- **A.** Deny permission to upload an object if the header does not include x-amz-server-side-encryption ✔
- **B.** Deny permission to upload an object if the header includes x-amz-server-side-encryption
- **C.** Deny permission to upload an object if the header does not include x-allow-encryption
- **D.** Deny permission to upload an object if the header includes x-allow-encryption

Explanation :

Answer - A
This is also given in the AWS Documentation

If you need server-side encryption for all of the objects that are stored in a bucket, use a bucket policy. For example, the following bucket policy denies permissions to upload an object unless the request includes the `x-amz-server-side-encryption` header to request server-side encryption:

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    }
  ]
}
```

Since the documentation clearly mentions what is the requirement for encryption to upload objects, all other options are invalid.

For more information on Server-Side Encryption , please refer to the below URL

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

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14846)

Certification

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

Company

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

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

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

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

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

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