DIAGNOSTIC TEST

Attempt 1

Marks Obtained 0 / 80

Your score is 0.0%

Completed on Tuesday , 29 January 2019 , 01:57 PM

Time Taken 00 H 00 M 46 S

Result Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Costing	9	0	1	8
2	Network Design	10	0	0	10
3	Security	20	0	0	20
4	Data Storage	7	0	0	7
5	Deployment Management	13	0	0	13
6	Cloud Migration & Hybrid Architecture	7	0	0	7
7	High Availability and Business Continuity	11	0	0	11
8	Scalability & Elasticity	3	0	0	3

80 Questions	0 Correct	1 Incorrect	79 Unattempted

Show Answers: All

QUESTION 1 INCORRECT COSTING

Your company asked you to create a mobile application. The application is built to work with DynamoDB as the backend and Javascript as the frontend. During the usage of the application, you notice that there are spikes in the application, especially in the DynamoDB area. Which option provides the most cost-effective and scalable architecture for this application? Choose an answer from the options below.

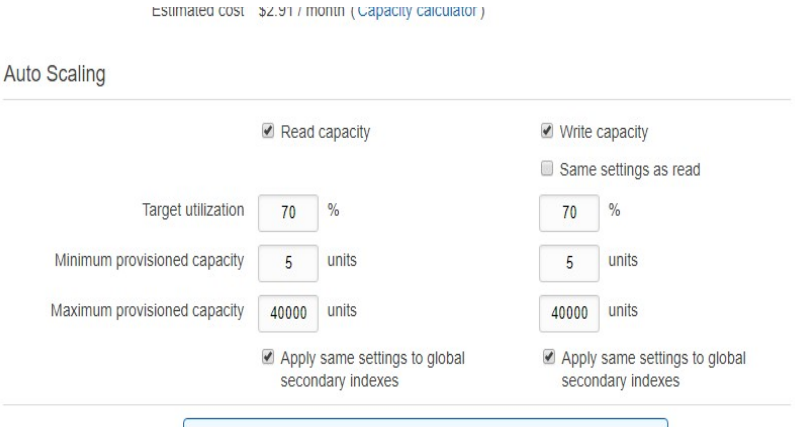
- **A.** Autoscale DynamoDB to meet the requirements. ✔
- **B.** Increase write capacity of DynamoDB to meet the peak loads.
- **C.** Create a service that pulls SQS messages and writes these to DynamoDB to handle sudden spikes in DynamoDB. ✖
- **D.** Launch DynamoDB in Multi-AZ configuration with a global index to balance writes.

Explanation :

Answer – A

DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read and write capacity to handle sudden increases in traffic, without throttling. When the workload decreases, Application Auto Scaling decreases the throughput so that you don't pay for unused provisioned capacity.

So in this case Option A is the correct answer.



For more details, please check below AWS Docs:

- https://aws.amazon.com/blogs/aws/new-auto-scaling-for-amazon-dynamodb/ (https://aws.amazon.com/blogs/aws/new-auto-scaling-for-amazon-dynamodb/)
- https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html)

Option B is incorrect because even though increasing the write capacity would solve the issue, it is not cost efficient.

Option C is incorrect as SQS is not a scaling solution but it can be used for decoupling and fault tolerance.

Ask our Experts

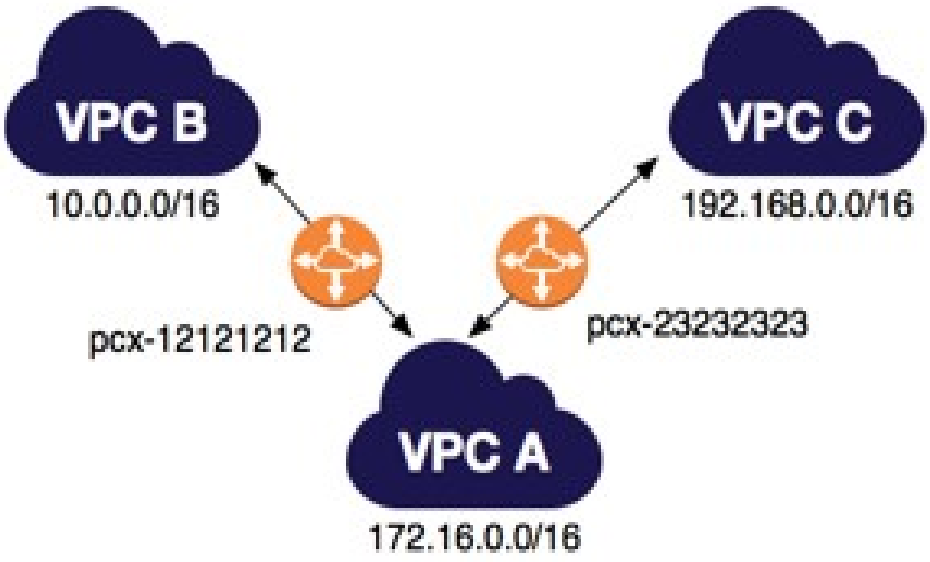
There are 2 companies that have their own AWS accounts. How can they connect to a central VPC for identity validation? How would you best design this solution? Choose an answer from the options below

- **A.** Migrate each VPC resources to the central VPC using migration tools such as Import/Export, Snapshot, AMI Copy, and S3 sharing.
- **B.** Create a VPC peering connection with the central VPC ✔
- **C.** Create a Direct Connect connection from each VPC endpoint to the central VPC.
- **D.** Create an OpenVPN instance in central VPC and establish an IPSec tunnel between VPCs.

Explanation :

Answer – B

Option A is incorrect because each VPC has its own purpose (responsibility) and setting of the resources inside - such as NACL, Security Groups, EC2 instances, NAT Instance/Gateway, Routing Tables etc., So merging into single VPC would defeat its purpose.
Option B is CORRECT because VPC peering allows the resources in peer VPCs to communicate with each other and in this case, can validate the identities of the resources. See the image below. Also, VPCs from different regions can be peered as well (Inter-Region VPC Peering).
Option C is incorrect because Direct Connect should be used when there is a need for dedicated connection between a customer data center and AWS/VPC.
Option D is incorrect because VPN should be used when there is a need for connecting customer data center to AWS/VPC resources via customer gateway.



More information on VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an *inter-region* VPC peering connection).
For more information on VPC Peering please see the below link
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html)
https://aws.amazon.com/blogs/aws/new-almost-inter-region-vpc-peering/
(https://aws.amazon.com/blogs/aws/new-almost-inter-region-vpc-peering/)

Ask our Experts

QUESTION 3 UNATTEMPTED SECURITY

As AWS grows, most of your clients' main concerns seem to be about security, especially when all of their competitors also seem to be using AWS. One of your clients asks you whether having a competitor who hosts their EC2 instances on the same physical host would make it easier for the competitor to hack into the client's data. Which of the following statements would be the best choice to put your client's mind at rest?

- **A.** Different instances running on the same physical machine are isolated from each other via a 256- bit Advanced Encryption Standard (AES-256).
- **B.** Different instances running on the same physical machine are isolated from each other via the Xen hypervisor and via a 256-bit Advanced Encryption Standard (AES-256).
- **C.** Different instances running on the same physical machine are isolated from each other via the Xen hypervisor. ✔
- **D.** Different instances running on the same physical machine are isolated from each other via IAM permissions.

Explanation :

Answer - C

Options A and B are incorrect because 256-bit AES is used for encrypting the data. Ensuring the isolation of the VMs running on a hypervisor is not its responsibility.
Option C is CORRECT because it is the hypervisor that hosts the VMs responsible for ensuring that the VMs are isolated from each other despite being hosted on the same underlying hypervisor.
Option D is incorrect because IAM permissions has nothing to do with the isolation of the VMs running on a hypervisor.

More information on this topic:

The shared responsibility model for infrastructure services, such as Amazon Elastic Compute Cloud (Amazon EC2) for example, specifies that AWS manages the security of the following assets:
• Facilities
• Physical security of hardware
• Network infrastructure
• Virtualization infrastructure
https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf
(https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf)

Ask our Experts

QUESTION 4 UNATTEMPTED SECURITY

You are building a large-scale confidential documentation web server on AWS, and all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use CloudFront to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below

- **A.** Create an Identity and Access Management (IAM) user for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- **B.** Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI. ✔
- **C.** Create individual policies for each bucket that stores documents and in that policy grant access to only CloudFront.
- **D.** Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

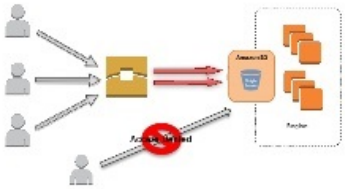
Explanation :

Answer – B

There are two main points (1) the files should not be accessed directly via S3 as they are confidential, and (2) the files should be accessible via CloudFront.
If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket, you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if users access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront access logs are less useful because they're incomplete. See the image below:

Control Access to Content on Amazon S3

- Origin Access Identity (OAI)
- Content can be accessed ONLY via CloudFront
- Why use OAI?
  - Ensures content is not leaking
  - S3 URLs not being used anywhere



Option A is incorrect because it does not give CloudFront the exclusive access to S3 bucket.
Option B is CORRECT because it gives CloudFront the exclusive access to S3 bucket, and prevents other users from accessing the public content of S3 directly via S3 URL.
Option C is incorrect because you do not need to create any individual policies for each bucket.
Option D is incorrect because (a) creating a bucket policy is unnecessary and (b) it does not prevent other users from accessing the public content of S3 directly via S3 URL.

For more information on Origin Access Identity, please see the below link
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html
(http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html)

Ask our Experts

QUESTION 5 UNATTEMPTED SECURITY

A customer is running a multi-tier web application farm in a virtual private cloud (VPC) that is not connected to their corporate network. They are connecting to the VPC over the Internet to manage all of their Amazon EC2 instances running in both the public and private subnets. They have only authorized the bastion-security-group with Microsoft Remote Desktop Protocol (RDP) access to the application instance security groups, but the company wants to further limit administrative access to all of the instances in the VPC. Which of the following Bastion deployment scenarios will meet this requirement?

- **A.** Deploy a Windows Bastion host on the corporate network that has RDP access to all instances in the VPC.
- **B.** Deploy a Windows Bastion host with an Elastic IP address in the public subnet and allow SSH access to the bastion from anywhere.
- **C.** Deploy a Windows Bastion host with an Elastic IP address in the private subnet, and restrict RDP access to the bastion from only the corporate public IP addresses.
- **D.** Deploy a Windows Bastion host with an auto-assigned Public IP address in the public subnet, and allow RDP access to the bastion from only the corporate public IP addresses. ✔

Explanation :

Answer - D

Option A is incorrect because a bastion host is deployed into the public subnet of a VPC with an Elastic IP address to allow inbound Secure Shell (SSH) access to EC2 instances in public and private subnets.

Option B is incorrect because the access should be RDP, not SSH, since the bastion host is a Windows machine.

Option C is incorrect because the bastion host needs to be placed in the public subnet, not private.

Option D is CORRECT because (a) it places the bastion host in the public subnet, and (b) only the corporate IP addresses has RDP access to it.

For more information on controlling network access to EC2 instances using a bastion server, please see the link below:

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

Ask our Experts

QUESTION 6 UNATTEMPTED DATA STORAGE

You have been tasked with creating file level restore on your EC2 instances. You already have the access to all the frequent snapshots of the EBS volume. You need to be able to restore an individual lost file on an EC2 instance within 15 minutes of a reported loss of information. The acceptable RPO is several hours. How would you perform this on an EC2 instance? Choose an answer from the options below

- **A.** Setup a cron that runs aws s3 cp on the files and copy the files from the EBS volume to S3

- **B.** Turn off the frequent snapshots of EBS volumes. Create a volume from an EBS snapshot, attach the EBS volume to the EC2 instance at a different mount location, cutover the application to look at the new backup volume and remove the old volume
- **C.** Create a volume from the source snapshot and attach the EBS volume to the same EC2 instance at a different mount location, browse the file system on the newly attached volume and select the file that needs to be restored, copy it from the new volume to the original source volume. ✔
- **D.** Enable auto snapshots on Amazon EC2 and restore the EC2 instance upon single file failure

Explanation :

Answer – C

Option A is incorrect because there is an assumption that the EC2 instance can read files from S3.
Option B is incorrect because the old volume that is connected to the EC2 could have different files compared to the snapshot that we are recovering from (i.e. some files may have been removed, some may have been newly added). If that volume is removed, we may lose some files and the final volume will not be in latest state. So, the best solution is to just copy the file from the recovery volume, and add it to the old connected/backup volume.
Option C is CORRECT because it mounts the EBS snapshot - that contains the file - as a volume and copies the file to the already attached volume. This way, the already attached volume always stays up-to-date. Once the file is copied, the volume - that was attached for copying the file - can be removed.
Option D is invalid because Amazon Data Lifecycle Manager (Amazon DLM) is used to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes. But for restoring a single file, we can mount the volume created from a snapshot to another mount location of the same EC2 instance and copy the file across to the initial volume from where the file is deleted.

For more information on EBS snapshots please visit the below URL
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)

Ask our Experts

QUESTION 7 UNATTEMPTED DATA STORAGE

Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets. Each collar will push 30kb of biometric data in JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending information back to the pet owners and veterinarians via a web portal. Management has tasked you to architect the collection platform ensuring the following requirements are met -

Provide the ability for real-time analytics of the inbound biometric data

Ensure that the processing of the biometric data is highly durable, elastic and parallel

The results of the analytic processing should be persisted for data mining

Which architecture outlined below win meet the initial requirements for the collection platform?

- **A.** Utilize S3 to collect the inbound sensor data analyze the data from S3 with a daily scheduled Data Pipeline and save the results to a Redshift Cluster.
- **B.** Utilize Amazon Kinesis to collect the inbound sensor data, analyze the data with Kinesis clients and save the results to a Redshift cluster using EMR. ✔
- **C.** Utilize S3 to collect the inbound sensor data analyze the data from SQS with Amazon Kinesis and save the results to a Microsoft SQL Server RDS instance.
- **D.** Utilize EMR to collect the inbound sensor data, analyze the data from EUR with Amazon Kinesis and save me results to DynamoDB.

Explanation :

Answer - B

The main point to consider here is that the information is to be analyzed in real-time, the solution should be highly durable, elastic and be processed in parallel, and the result should be persisted for data mining after the analysis. Whenever the question requires real-time processing of data, always think about using Amazon Kinesis!
Option A is incorrect because (a) S3 is not efficient for collecting and storing real-time data, and (b) daily scheduled data pipeline is not a real-time analytics solution.
Option B is CORRECT because (a) Amazon Kinesis is ideal for capturing and processing real-time data captured by the sensor, (b) it also stores the result of analysis later, and (c) Redshift cluster can be used for processing (data mining) the information captured by the Kinesis and copied via EMR.
Option C is incorrect because (a) S3 is not efficient for collecting and storing real-time data, and (b) MSSQL Server RDS is not ideal for storing the information for data mining.
Option D is incorrect because (a) EMR alone is not ideal to capture data and would need specific frameworks like Kafka to capture data for processing. Also, real-time analytics needs to done using Spark Streaming and not EMR alone, and (b) DynamoDB is not used for data mining.
More information on Amazon Kinesis with Redshift:
https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html
(https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html)

Ask our Experts

QUESTION 8 UNATTEMPTED DEPLOYMENT MANAGEMENT

A legacy software is hosted on an EC2 instance which has the license tied to the MAC address. From your experience with AWS, you know that every time an instance is restarted, it will almost certainly lose it's MAC address. What will be a possible solution to this? Choose an answer from the options below

- **A.** Make sure that EC2 Instance you deploy has a static IP address that is mapped to the MAC address.
- **B.** Use a VPC with a private subnet for the license and a public subnet for the EC2.
- **C.** Use a VPC with a private subnet and configure the MAC address to be tied to that subnet.
- **D.** Use a VPC with an elastic network interface that has a fixed MAC Address. ✔

Explanation :

Answer – D

Option A is incorrect because you cannot map a static IP address to a MAC address.
Option B is incorrect because putting license server in private subnet would not resolve the dependency on the license that is based on a MAC address.
Option C is incorrect because MAC addresses cannot be tied to subnets.
Option D is CORRECT because you should use Elastic Network Interface that is associated with a fixed MAC address. This will ensure that the legacy license based software would always work and not lose the MAC address any point in future.

For more information on elastic network interfaces please visit the below URL
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html)

Ask our Experts

QUESTION 9 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

Your final task, that will complete a cloud migration for a customer, is to set up an Active Directory service for them so that they can use Microsoft Active Directory with the newly-deployed AWS services. After reading the AWS documentation for this, you discover that three options are available to set up the AWS Directory

Service. You call the customer to collect more information about their requirements, and they tell you that they have 1,000 users on their AD service and want to be able to use their existing on-premises directory with AWS services.

Which of the following options would be the most appropriate to set up the AWS Directory Service for your customer?

- **A.** Simple AD
- **B.** AWS Directory Service for Microsoft Active Directory (Enterprise Edition)
- **C.** AD Connector ✔
- **D.** Any of these options are acceptable as long as they configured correctly for 1,000 customers.

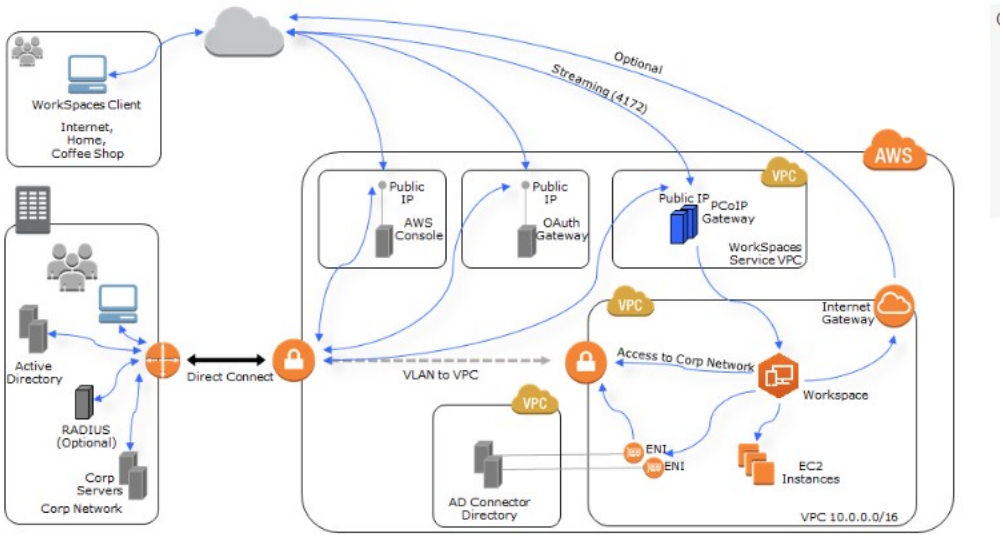
Explanation :

Answer – C

For the exam, remember the usage of the following AD options:

- SimpleAD: Microsoft Active Directory compatible directory from AWS Directory Service and supports common features of an active directory.
- AWS Directory Service for Microsoft Active Directory: Managed Microsoft Active Directory that is hosted on AWS cloud.
- AD Connector: Proxy service for connecting your on-premises Microsoft Active Directory to the AWS cloud.

Option A is incorrect because SimpleAD does not connect existing on-premises AD to AWS.
Option B is incorrect because AWS Directory Service for Microsoft AD is an AWS managed service that is hosted on the AWS cloud, it does not connect your AD with AWS.
Option C is CORRECT because AD Connector helps connecting your on-premises Microsoft Active Directory to the AWS cloud.
Option D is incorrect because none of the options above are acceptable except AD Connector.



For an example of setup of AD connector, please visit the below URL:

- https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/architecture.html (https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/architecture.html)

Ask our Experts

QUESTION 10 UNATTEMPTED COSTING

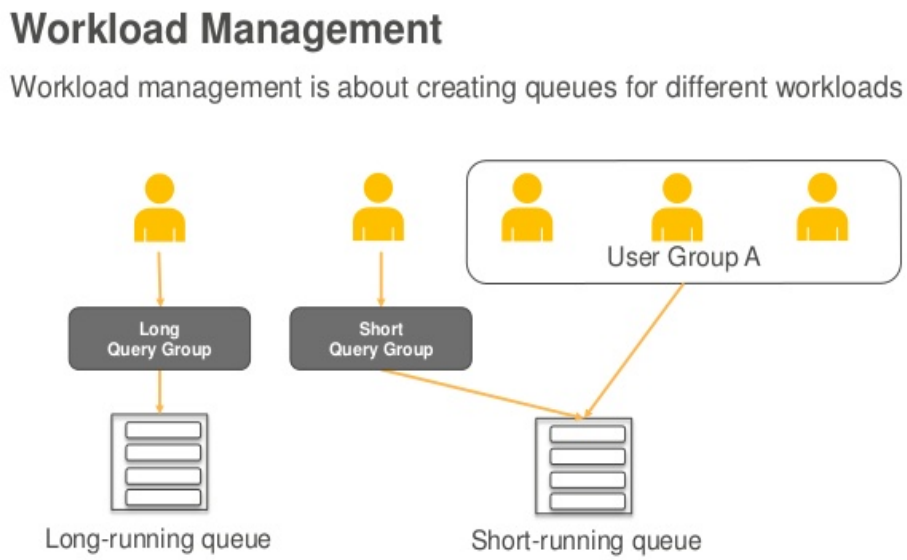
You have two different groups to analyze data of a petabyte-scale data warehouse using Redshift. Each query issued by the first group takes approximately 1-2 hours to analyze the data while the second group's queries only take between 5-10 minutes to analyze data. You don't want the second group's queries to wait until the first group's queries are finished. You need to design a solution so that this does not happen. Which of the following will be the best and cheapest solution to solve this dilemma? Choose an answer from the options below:

- **A.** Create a read replica of Redshift and run the second team's queries on the read replica.
- **B.** Create two separate workload management groups and assign them to the respective groups. ✔
- **C.** Pause the long queries when necessary and resume them when no query is running.
- **D.** Start another Redshift cluster from a snapshot for the second team if the current Redshift cluster is busy processing long queries.

Explanation :

Answer – B
Whenever the question gives you scenario where, in Redshift, there are two processes - one fast and one slow, and you are asked to ensure that there is no impact on the queries of a process, always think about creating two separate workload management groups.

Option A is incorrect because Redshift does not have read replicas.
Option B is CORRECT because the best solution - without any effect on performance - is to create two separate workload management groups - one for each department and run the queries on them. See the image below.
Option C is incorrect because queries cannot be paused in Redshift.
Option D is incorrect because this will affect the performance of the current Redshift cluster.



More information on Amazon Redshift Workload Management
Amazon Redshift workload management (WLM) enables users to manage priorities flexibly within workloads so that short, fast-running queries won't get stuck in queues behind long-running queries. Amazon Redshift WLM creates query queues at runtime according to service classes, which define the configuration parameters for various types of queues, including internal system queues and user-accessible queues. From user's perspective, a user-accessible service class and a queue are functionally equivalent. For consistency, this documentation uses the term queue to mean a user-accessible service class as well as a runtime queue.
For more information on redshift workload management, please refer to the below URL
http://docs.aws.amazon.com/redshift/latest/dg/c_workload_mngmt_classification.html
(http://docs.aws.amazon.com/redshift/latest/dg/c_workload_mngmt_classification.html)

Ask our Experts

QUESTION 11 UNATTEMPTED SECURITY

You have just developed a new mobile application that handles analytics workloads on large-scale datasets that are stored on Amazon Redshift. Consequently, the application needs to access Amazon Redshift tables. Which of the following methods would be the best, both practically and security-wise, to access the tables? Choose the correct answer from the options below

- **A.** Create an IAM user and generate encryption keys for that user. Create a policy for Redshift read-only access. Embed the keys in the application.
- **B.** Create a HSM client certificate in Redshift and authenticate using this certificate.
- **C.** Create a Redshift read-only access policy in IAM and embed those credentials in the application.
- **D.** Use roles that allow a web identity federated user to assume a role that allows access to the Redshift table by providing temporary credentials. ✔

Explanation :

Answer – D

Tip: When a service, user, or application needs to access any AWS resource, always prefer creating an IAM Role over creating an IAM User.

Option A is incorrect because embedding keys in the application to access AWS resource is not a good architectural practice as it creates security concerns.
Option B is incorrect because HSM certificate is used by Redshift cluster to connect to the client's HSM in order to store and retrieve the keys used to encrypt the cluster databases.
Option C is incorrect because read-only policy is insufficient and embedding keys in the application to access AWS resource is not a good architectural practice as it creates security concerns.
Option D is CORRECT because (a) IAM role allows the least privileged access to the AWS resource, (b) web identity federation ensures the identity of the user, and (c) the user is given temporary credentials to access the AWS resource.

For more information on IAM policies please refer to the below link:
http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)
For more information on web identity federation please refer to the below link:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

Ask our Experts

QUESTION 12 UNATTEMPTED DATA STORAGE

Your company has HQ in Tokyo and branch offices all over the world and is using a logistics software with a multi-regional deployment on AWS in Japan, Europe and USA. The logistic software has a 3-tier architecture and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database. In the HQ region you run an hourly batch process reading data from every region to compute cross-regional reports that are sent by email to all offices. This batch process must be completed as fast as possible, to quickly optimize logistics. How do you build the database architecture in order to meet the requirements?

- **A.** For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files hourly to the HQ region.
- **B.** For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS snapshots to the HQ region.
- **C.** For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS snapshots to the HQ region.
- **D.** For each regional deployment, use RDS MySQL with a master in the region and a read replica in the HQ region. ✔
- **E.** Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network latency for the batch process.

Explanation :

Answer - D

The problem in the scenario is that, currently, an hourly batch process is run at the HQ region that reads the data from every region to compute cross-regional reports. This is a slow process and need to be quickened. The most ideal scenario would be to have the replicated database in

Option A is incorrect because copying the data hourly to HQ region would be slow compared to the best option, which is D.

Option B is incorrect because (a) taking hourly EBS snapshots would affect the performance of the database in its master region, and (b) copying the snapshots hourly across the region would be a slow process.

Option C is incorrect because (a) taking hourly RDS snapshots would affect the performance of the database in its master region, and (b) sending the snapshots hourly across the region would be a slow and very costly process.

Option D is CORRECT because (a) it creates a read replica in the HQ region which is updated asynchronously. This way, generating the reports would be very quick, and (b) it does not affect the performance of the databases in their respective master region.

Option E is incorrect because AWS Direct Connect is very expensive option and it would take considerable time to setup.

For more information on cross-region read replicas, please visit the link below:

https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/ (https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/)

Ask our Experts

QUESTION 13 UNATTEMPTED DEPLOYMENT MANAGEMENT

A legacy application with licensing is attached to a single MAC address. Since an EC2 instance can receive a new MAC address while launching new instances. How can you ensure that your EC2 instance can maintain a single MAC address for licensing? Choose the correct answer from the options below:

- **A.** Create an ENI and assign it to the EC2 instance. The ENI will have a static MAC address and can be detached and reattached to a new instance if the current instance becomes unavailable. ✔
- **B.** Private subnets have static MAC addresses. Launch the EC2 instance in a private subnet and, if required, use a NAT to serve data over the internet.
- **C.** Configure a manual MAC address for each EC2 instance and report that to the licensing company.
- **D.** AWS cannot have a fixed MAC address; the best solution is to create a dedicated VPN/VGW gateway to serve data from the legacy application.

Explanation :

Answer – A
Tip: Whenever a question has a scenario where you need to use fixed MAC address for EC2 instances, always think about using Elastic Network Interface (ENI).
If a static MAC address is assigned to an ENI, it remains unchanged. As long as the EC2 has that ENI, it's MAC address will not change.

Option A is CORRECT because, as mentioned above, as ENI with static MAC address can be assigned to the EC2 instance. If the instance becomes unavilable or needs to be replaced, the ENI can be detached and re-attached to another EC2 while maintaining the same MAC address.
Option B is incorrect because subnets have CIDR, not static MAC addresses.
Option C is incorrect because if the EC2 instance fails or becomes unavailable, its MAC address cannot be reused with another EC2 instance.
Option D is incorrect because you can avail ENI in order to have static MAC address for the EC2 instances.

More information on ENI on AWS Documentation:
Create a Low Budget High Availability Solution
If one of your instances serving a particular function fails, its network interface can be attached to a replacement or hot standby instance pre-configured for the same role in order to rapidly recover the service. For example, you can use a network interface as your primary or secondary network interface to a critical service such as a database instance or a NAT instance. If the instance fails, you (or more

likely, the code running on your behalf) can attach the network interface to a hot standby instance. Because the interface maintains its private IP addresses, Elastic IP addresses, and MAC address, network traffic begins flowing to the standby instance as soon as you attach the network interface to the replacement instance. Users experience a brief loss of connectivity between the time the instance fails and the time that the network interface is attached to the standby instance, but no changes to the VPC route table or your DNS server are required.
Best Practices for Configuring Network Interfaces
For more information on elastic network interfaces please visit the below URL

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html)

Ask our Experts

QUESTION 14 UNATTEMPTED NETWORK DESIGN

Your company has just set up a new document server on its AWS VPC, and it has four very important clients that it wants to give access to. These clients also have VPCs on AWS and it is through these VPCs that they will be given access to the document server. In addition, each of the clients should not have access to any of the other clients' VPCs. Choose the correct answer from the options below

- **A.** Set up VPC peering between your company's VPC and each of the clients' VPCs. ✔
- **B.** Set up VPC peering between your company's VPC and each of the clients' VPCs, but block the IPs from CIDR of the clients' VPCs to deny access between each other.
- **C.** Set up VPC peering between your company's VPC and each of the clients' VPC. Each client should have VPC peering set up between each other to speed up access time.
- **D.** Set up all the VPCs with the same CIDR but have your company's VPC as a centralized VPC.

Explanation :

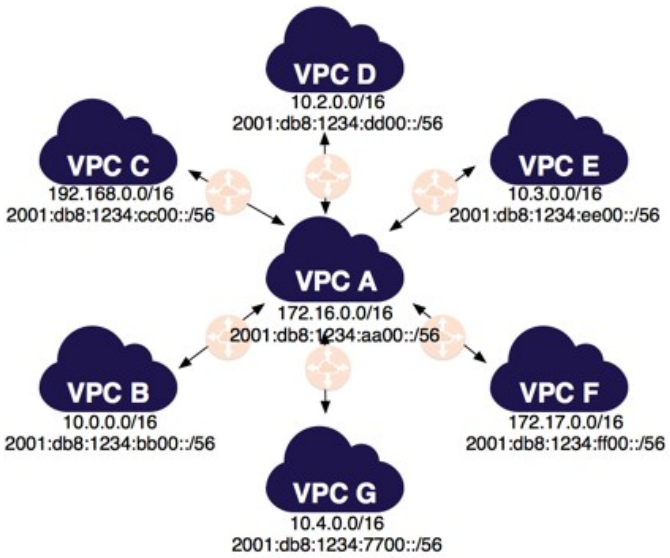
Answer – A
In this scenario, you are asked how resources from 4 VPCs can access resources from another VPC. This is a use case of "Star-Shaped" VPC peering shown in the image below. In this configuration, VPCs that have non-overlapping CIDR with your VPC, are peered for the intent of accessing the resources using their private IP addresses.

- Option A is CORRECT because, as mentioned above, the peered VPCs can share and access the resources within each other via their private IP addresses.
- Option B is incorrect because you do not need to block any IP addresses in this scenario.
- Option C is incorrect because the peering among the client VPCs is unnecessary. The only peering that is needed is between each client and your VPC.
- Option D is incorrect because, for VPC Peering, the VPCs should not have overlapping CIDRs. So, VPCs having the same CIDR cannot be peered.

For more information on VPC Peering please see the below link

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

Note:
The scenario in question is describing an architecture similar to the one given below:



VPC A id your company and the rest of the other 6 companies are your clients and you have set up separate VPC peering connection with each of your client allowing only them to have communication with your company VPC.
In the above configuration VPC D can communicate with VPC A. VPC B can communicate with VPC A, but VPC D cannot communicate with VPC B through VPC peering connection.

Ask our Experts

QUESTION 15 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

A company has a library of on-demand MP4 files needing to be streamed publicly on their new video webinar website. The video files are archived and are expected to be streamed globally, primarily on mobile devices. Which of the following architectures can be implemented as a solution to this requirement.
Select 2 answers.

- [ ] **A.** Provision streaming EC2 instances which use S3 as the source for the HLS on-demand transcoding on the servers. Provision a new CloudFront streaming distribution with the streaming server as the origin.
- [ ] **B.** Provision streaming EC2 instances which use S3 as the source for the HLS on-demand transcoding on the servers. Provision a new CloudFront download distribution with the WOWZA streaming server as the origin. ✔
- [ ] **C.** Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and create an on-demand video streaming CloudFront distribution with download option to serve the HLS file to end users. ✔
- [ ] **D.** Upload the MP4 files to S3 and create an Elastic Transcoder job that transcodes the MP4 source into HLS chunks. Store the HLS output in S3 and create an RTMP CloudFront distribution with a live video streaming option to stream the video contents.?

Explanation :

Answer – B and C

Tip: In exam, if the question presents a scenario, where the media is to be streamed globally in MP4 format, on multiple platform devices, always think about using Elastic Transcoder.
Option A is incorrect because (a) provisioning of streaming EC2 instances is a costly solution, (b) the videos are to be delivered on-demand, not live streaming.
Option D is incorrect because both these options support live streaming and not on-demand streaming.
Option B is correct.
It is possible to deliver both live stream and on-demand video streaming with AWS and Wowza. But there will be a latency when delivering through CloudFront although in most cases, the latency is within acceptable ranges.

For more Information, please check below AWS Docs:
https://www.wowza.com/resources/webinars/aws-video-streaming
(https://www.wowza.com/resources/webinars/aws-video-streaming)
https://www.wowza.com/products/streaming-engine/deployment-options/aws
(https://www.wowza.com/products/streaming-engine/deployment-options/aws)
Option C is CORRECT because it (a) it uses Elastic Transcoder for transcoding the videos to different formats, (b) it uses CloudFront distribution with download option for streaming the on demand videos using HLS on any mobile, and (c) it uses S3 as origin, so keeps the cost low.
In the on demand streaming case, your video content is stored in Amazon S3. Viewers can choose to watch it at any desired time. A complete on-demand streaming solution typically makes use of Amazon S3 for storage, AWS Elemental MediaConvert for file-based video processing, and Amazon CloudFront for delivery.
Once uploaded, you may need to convert your video into the size, resolution, or format needed by a particular television or connected device. AWS Elemental MediaConvert will take care of this for you. MediaConvert takes content from S3, transcodes it per your request, and stores the result back in S3. Transcoding processes video files, creating compressed versions of the original content to reduce its size, change its format, or increase playback device compatibility.You can also create assets that vary in resolution and bitrate for adaptive bitrate streaming, which adjusts the viewing quality depending on

the viewer's available bandwidth. AWS Elemental MediaConvert outputs the transcoded video to an S3 bucket.
The next step is global delivery with Amazon CloudFront. CloudFront caches content at the edges for low latency and high throughput video delivery. This delivery can be made in two different ways. You can deliver the entire video file to the device before playing it, or you can stream it to the device.

More information is available at:
https://aws.amazon.com/cloudfront/streaming/ (https://aws.amazon.com/cloudfront/streaming/)
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-video.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-video.html)

More information on Elastic Transcoder:
Amazon Elastic Transcoder manages all aspects of the media transcoding process for you transparently and automatically. There's no need to use administer software, scale hardware, tune performance, or otherwise manage transcoding infrastructure. You can simply create a transcoding "job" specifying the location of your source media file and how you want it transcoded. Amazon Elastic Transcoder also provides transcoding presets for popular output formats, which means that you don't need to guess about which settings work best on particular devices.
For more information on Elastic transcoder, please see the below link
https://aws.amazon.com/elastictranscoder/ (https://aws.amazon.com/elastictranscoder/)

Ask our Experts

QUESTION 16 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

A company needs to configure a NAT instance for its internal AWS applications to be able to download patches and package software. Currently, they are running a NAT instance that is using the floating IP scripting configuration to create fault tolerance for the NAT. The NAT instance needs to be built with fault tolerance in mind. What is the best way to configure the NAT instance with fault tolerance?

Choose the correct answer from the options below:

- **A.** Create one NAT instance in a public subnet; create a route from the private subnet to the NAT instance
- **B.** Create two NAT instances in a public subnet; create a route from the private subnet to each NAT instance for fault tolerance.
- **C.** Create a NAT instance in a public subnet with application running in private subnet in an AZ. Create a similar architecture in another AZ; create a route from the private subnet to each NAT instance residing in these AZ's for fault tolerance. ✔
- **D.** Create two NAT instances in two separate private subnets.

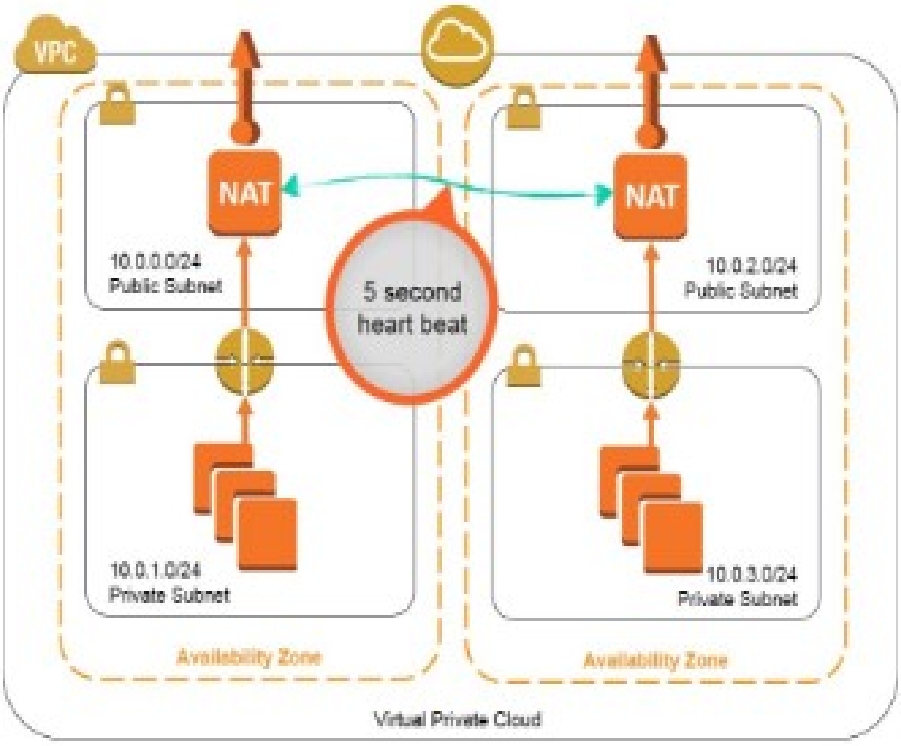
Explanation :

Answer – C

- Option A is incorrect because you would need at least two NAT instances for fault tolerance.

- Option B is incorrect because if you put both NAT instances in a single public subnet and that subnet becomes unavailable or unreachable to the other instances, the architecture would not be fault tolerant.
- Option C is CORRECT because you should place two NAT instances in two separate public subnets, and create route from instances via each NAT instance for achieving fault tolerance.
- Option D is incorrect because you should not be putting the NAT instances in private subnet as they need to communicate with the internet. They should be in public subnet.

More information on NAT instances:
One approach to this situation is to leverage multiple NAT instances that can take over for each other if the other NAT instance should fail. This walkthrough and associated monitoring script (nat_monitor.sh) provide instructions for building an HA scenario where two NAT instances in separate Availability Zones (AZ) continuously monitor each other. If one NAT instance fails, this script enables the working NAT instance to take over outbound traffic and attempts to fix the failed instance by stopping and restarting it.
Below is a diagram for fault tolerant NAT instances.



For more information on fault-tolerant NAT gateways please see the below link

- https://aws.amazon.com/articles/2781451301784570 (https://aws.amazon.com/articles/2781451301784570)

Ask our Experts

QUESTION 17 UNATTEMPTED NETWORK DESIGN

When you create a subnet, you specify the CIDR block for the subnet. The CIDR block of a subnet can be the same as the CIDR block for theVPC (for a single subnet in the VPC) or a subset (to enable multiple subnets). The allowed block sizeis between a /28 netmask and /16 netmask. What is the maximum and minimum number of IP addresses according to AWS? You have also created a VPC with CIDR block of 10.0.0.0./24. How many IP addresses are supported by this VPC that can be allocated to various resources with in the VPC?

- **A.** Maximum is 28 and minimum is 16. The number of IP addresses that we can use with in this VPC is 24.
- **B.** Maximum is 256 and minimum is 16. The number of IP addresses that we can use with in this VPC is 123.
- **C.** Maximum is 65536 and minimum is 24. The number of IP addresses that we can use with in this VPC is 19.
- **D.** Maximum is 65536 and minimum is 16. The number of IP addresses that we can use with in this VPC is 251. ✔

Explanation :

Answer – D

First let us calculate the current number of IP addresses. The CIDR block is 10.0.0.0/24. Hence, out of 32 bits of address, 24 bits are set/masked. Hence, the remaining 8 bits indicate the remaining available IP addresses. Hence, the total number of current available instances is 2^(32-24) = 2^8 = 256.
Now, the maximum allowed block size is a /16 netmask. i.e. Out of 32, first 16 bits are set/masked, leaving 16 bits available. Hence, the total number of maximum available instances = 2^(32-16) = 2^16 = 65,536.
Now, the minimum allowed block size is a /28 netmask. i.e Out of 32, first 28 bits are set/masked, leaving 4 bits available. Hence, the total number of minimum available instances = 2^(32-28) = 2^4 = 16.

For more information on VPC and subnets please see the below link:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html)

5 IP addresses are reserved by AWS.
The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2 Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information,

see Amazon DNS Server (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#AmazonDNS).

- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

For More information, Please check below AWS Docs:

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

Ask our Experts

QUESTION 18 UNATTEMPTED SCALABILITY & ELASTICITY

A 3-tier e-commerce web application is current deployed on-premises and will be migrated to AWS for greater scalability and elasticity. The web server currently shares read-only data using a network distributed file system. The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast. The database tier uses shared-storage clustering to provide database failover capability, and uses several read slaves for scaling. Data on all servers and the distributed file system directory is backed up weekly to off-site tapes. Which AWS storage and database architecture meets the requirements of the application?

- **A.** Web servers store read-only data in S3, and copy from S3 to root volume at boot time. App servers share state using a combination of DynamoDB and IP unicast. Database use RDS with multi-AZ deployment and one or more Read Replicas. Backup web and app servers backed up weekly via AMIs, database backed up via DB snapshots. ✔
- **B.** Web servers store read-only data in S3, and copy from S3 to root volume at boot time. App servers share state using a combination of DynamoDB and IP unicast. Database use RDS with multi-AZ deployment and one or more Read replicas. Backup web servers app servers, and database backed up weekly to Glacier using snapshots.
- **C.** Web servers store read-only data in S3 and copy from S3 to root volume at boot time. App servers share state using a combination of DynamoDB and IP unicast. Database use RDS with multi-AZ deployment. Backup web and app servers backed up weekly via AMIs. Database backed up via DB snapshots.

- **D.** Web servers, store read-only data in an EC2 NFS server, mount to each web server at boot time. App servers share state using a combination of DynamoDB and IP multicast. Database use RDS with multi-AZ deployment and one or more Read Replicas. Backup web and app servers backed up weekly via AMIs, and database backed up via DB snapshots.

Explanation :

Answer - A

The main requirements of this scenario are: (1) the application should be scalable and elastic, (2) app servers should be able to share the state, (3) need read replicas, and (4) weekly backup of the data.

Option A is CORRECT because (a) the overall architecture is highly available, elastic, and scalable, (b) web servers share state using DynamoDB and IP unicast that is supported by AWS, (c) it supports read replicas, and (d) weekly backup for servers using AMIs and data using DB snapshots.

Option B is incorrect because you cannot backup data to Glacier using snapshots.

Option C is incorrect because it does not address the requirement of having read replicas for elasticity and scalability.

Option D is incorrect because AWS does not support IP multicast or broadcast.

For more information on this topic, please visit the links below:

https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf (https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf)

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

Ask our Experts

QUESTION 19 UNATTEMPTED SCALABILITY & ELASTICITY

You have a legacy application running that uses an m4.large instance size and cannot scale with Auto Scaling, but only has peak performance 5% of the time. This is a huge waste of resources and money so your Senior Technical Manager has set you the task of trying to reduce costs while still keeping the legacy application running as it should. Which of the following will best accomplish the task your manager has assigned you? Choose the correct answer from the options below:

- **A.** Use a T2 burstable performance instance. ✔
- **B.** Use a C4.large instance with enhanced networking.
- **C.** Use two t2.nano instances that have single Root I/O Virtualization.

- **D.** Use t2.nano instance and add spot instances when they are required.

Explanation :

Answer – A
The AWS documentation clearly indicates using T2 EC2 instance types for those instances which don't use CPU that often.
T2
T2 instances are Burstable Performance Instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
T2 Unlimited instances can sustain high CPU performance for as long as a workload needs it. For most general-purpose workloads, T2 Unlimited instances will provide ample performance without any additional charges. If the instance needs to run at higher CPU utilization for a prolonged period, it can also do so at a flat additional charge of 5 cents per vCPU-hour.
The baseline performance and ability to burst are governed by CPU Credits. T2 instances receive CPU Credits continuously at a set rate depending on the instance size, accumulating CPU Credits when they are idle, and consuming CPU credits when they are active. T2 instances are a good choice for a variety of general-purpose workloads including micro-services, low-latency interactive applications, small and medium databases, virtual desktops, development, build and stage environments, code repositories, and product prototypes. For more information see Burstable Performance Instances.
For more information on EC2 instance types please see the below link:
https://aws.amazon.com/ec2/instance-types/ (https://aws.amazon.com/ec2/instance-types/)

Ask our Experts

QUESTION 20 UNATTEMPTED NETWORK DESIGN

The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network. You can have multiple sets of DHCP options, but you can associate only one set of DHCP options with a VPC at a time. You have just created your first set of DHCP options, associated it with your VPC but now realize that you have made an error in setting them up and you need to change the options. Which of the following options do you need to take to achieve this? Choose the correct answer from the options below

- **A.** You need to stop all the instances in the VPC. You can then change the options, and they will take effect when you start the instances.
- **B.** You can modify the options from the console or the CLI.
- **C.** You must create a new set of DHCP options and associate them with your VPC. ✔
- **D.** You can modify the options from the CLI only, not from the console.

Explanation :

Answer – C
Option A, B, and D are incorrect because you cannot modify the DHCP options - neither via the

console nor via CLI.
Option C is CORRECT because once you create a set of DHCP options, you cannot modify them. You must create a new set of DHCP options and associate it with your VPC.
AWS Document says:
Changing DHCP Options
After you create a set of DHCP options, you can't modify them. If you want your VPC to use a different set of DHCP options, you must create a new set and associate them with your VPC. You can also set up your VPC to use no DHCP options at all.
You can have multiple sets of DHCP options, but you can associate only one set of DHCP options with a VPC at a time. If you delete a VPC, the DHCP options set associated with the VPC are also deleted.
After you associate a new set of DHCP options with a VPC, any existing instances and all new instances that you launch in the VPC use these options. You don't need to restart or relaunch the instances. They automatically pick up the changes within a few hours, depending on how frequently the instance renews its DHCP lease. If you want, you can explicitly renew the lease using the operating system on the instance.
For more information on DHCP Options set please see the below link:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html)

Ask our Experts

QUESTION 21 UNATTEMPTED SECURITY

The company you work for has a huge amount of infrastructure built on AWS. However, there has been some concerns recently about the security of this infrastructure, and an external auditor has been given the task of running a thorough check of all of your company's AWS assets. The auditor will be in the USA while your company's infrastructure resides in the Asia Pacific (Sydney) region on AWS. Initially, he needs to check all of your VPC assets, specifically, security groups and NACLs You have been assigned the task of providing the auditor with a login to be able to do this. Which of the following would be the best and most secure solution to provide the auditor with so he can begin his initial investigations? Choose the correct answer from the options below

- **A.** Create an IAM user tied to an administrator role. Also provide an additional level of security with MFA.
- **B.** Give him root access to your AWS Infrastructure, because he is an auditor he will need access to every service.
- **C.** Create an IAM Role with the read only permissions to access the AWS VPC infrastructure and assign that role to the auditor. ✔
- **D.** Create an IAM user with full VPC access but set a condition that will not allow him to modify anything if the request is from any IP other than his own.

Explanation :

Answer – C
Generally, you should refrain from giving high-level permissions and give only the required permissions. In this case, option C fits well by just providing the relevant access which is required.

- Option A is incorrect because you should create an IAM Role with the needed permissions.
- Option B is incorrect because you should not give the root access as it will give the user full access to all AWS resources.
- Option C is CORRECT because IAM Role gives just the minimum required permissions (read-only) to audit the VPC infrastructure to the auditor.
- Option D is incorrect because you should not give the auditor full access to the VPC.

For more information on IAM, please see the below link

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

Note:
IAM roles can be assigned to users as well. Please check the below link to know more about it.

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

Ask our Experts

QUESTION 22 UNATTEMPTED NETWORK DESIGN

You want to set up a public website on AWS. The things that you require are as follows:

- You want the database and the application server running on AWS VPC.

- You want the database to be able to connect to the Internet, specifically for any patch upgrades.

- You do not want to receive any incoming requests from the Internet to the database.

Which of the following solutions would be the best to satisfy all the above requirements for your planned public website on AWS? Choose the correct answer from the options below

○ **A.** Set up the database in a private subnet with a security group which only allows outbound traffic.

- **B.** Set up the database in a public subnet with a security group which only allows inbound traffic.
- **C.** Set up the database in a local data center and use a private gateway to connect the application to the database.
- **D.** Set up the public website on a public subnet and set up the database in a private subnet which connects to the Internet via a NAT instance. ✔

Explanation :

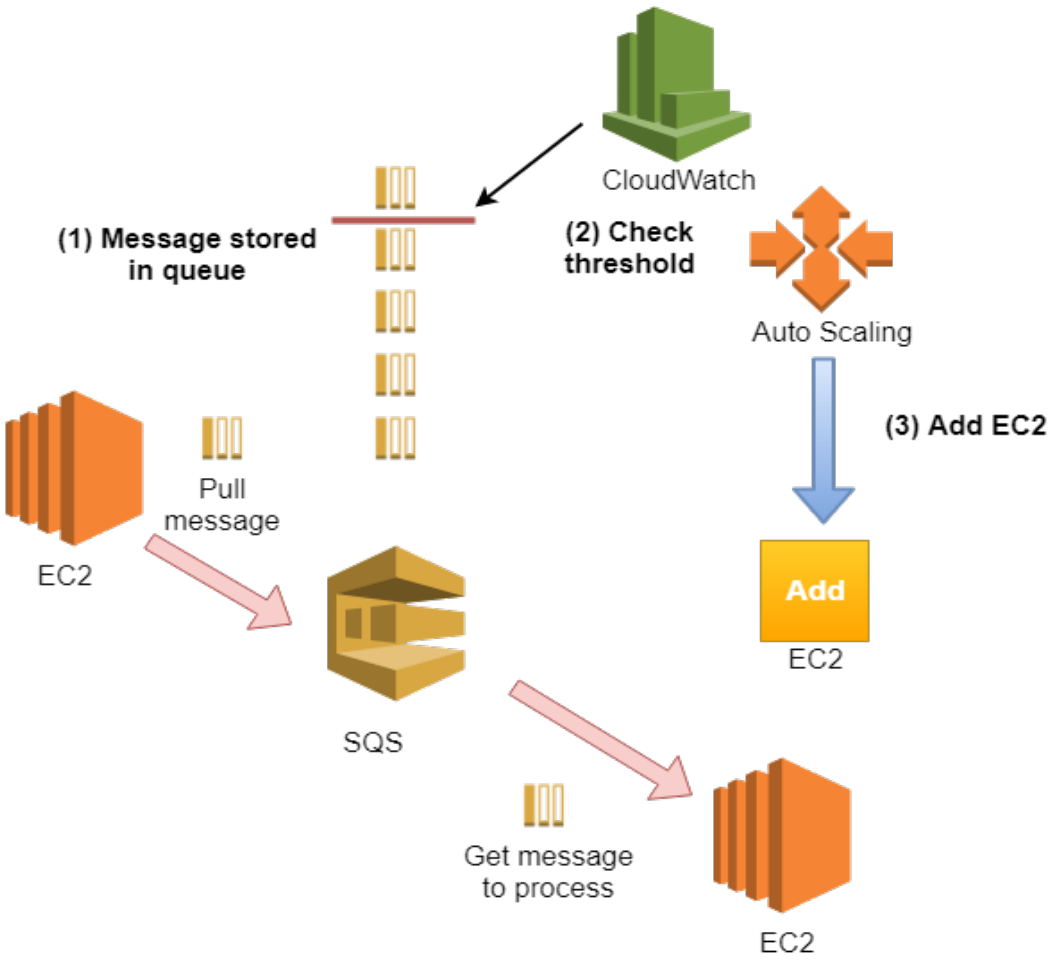
Answer – D

Option A is incorrect because you need NAT instance or NAT gateway in the public subnet to be able to download the required patches.
Option B is incorrect because (a) you need NAT instance or NAT gateway to be able to download the required patches, and (b) you cannot allow or deny only inbound traffic via security group as it is stateful.
Option C is incorrect because you do not need to set up any local data center.
Option D is CORRECT because you should set up the data server in private subnet as it needs only the traffic from NAT instance or NAT Gateway, and not from the internet.

For more information on the VPC Scenario for public and private subnets please see the below link
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts

QUESTION 23 UNATTEMPTED COSTING



Refer to the architecture diagram above of a batch processing solution using Simple Queue Service (SQS) to set up a message queue between EC2 instances which are used as batch processors. CloudWatch monitors the number of job requests (queued messages) and an Auto Scaling group adds or deletes batch servers automatically based on the parameters set in the CloudWatch alarms. You can use this architecture to implement which of the following features in a cost effective and efficient manner?

- **A.** Reduce the overall time for executing jobs through parallel processing by allowing a busy EC2 instance that receives a message to pass it to the next instance in a daisy-chain setup.
- **B.** Implement fault tolerance against EC2 instance failure since messages would remain in SQS and worn can continue with recovery of EC2 instances implement fault tolerance against SQS failure by backing up messages to S3.
- **C.** Implement message passing between EC2 instances within a batch by exchanging messages through SQS.

- **D.** Coordinate number of EC2 instances with number of job requests automatically thus improving cost effectiveness. ✔
- **E.** Handle high priority jobs before lower priority jobs by assigning a priority metadata field to SQS messages.

Explanation :

Answer - D

Option A is incorrect because the EC2 instances are part of auto scaling group and may be terminated based on the load. So, the messages cannot be passed amongst the instances in daisy-chain setup.

Option B is incorrect because it is not implementing any fault tolerance against SQS failure by backing up messages to S3.

Option C is incorrect because the messages cannot be passed amongst the instances as they are part of an auto scaling group and may be terminated based on the load.

Option D is CORRECT because the EC2 instances are created/terminated by auto scaling group based on the CloudWatch alarm that is triggered based on the threshold set on the number of messages in the SQS queue.

Option E is incorrect because there are no priority metadata fields in SQS messages.

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

Ask our Experts

QUESTION 24 UNATTEMPTED SECURITY

You're building a mobile application game. The application needs permissions for each user to communicate and store data in DynamoDB tables. What is the best method for granting each mobile device that installs your application to access DynamoDB tables for storage when required? Choose the correct answer from the options below

- **A.** During the install and game configuration process, each user create an IAM credential and assign the IAM user to a group with proper permissions to communicate with DynamoDB.
- **B.** Create an IAM group that only gives access to your application and to the DynamoDB tables. Then, when writing to DynamoDB, simply include the unique device ID to associate the data with that specific user.
- **C.** Create an IAM role with the proper permission policy to communicate with the DynamoDB table. Use web identity federation, which assumes the IAM role using AssumeRoleWithWebIdentity, when the user signs in, granting temporary security credentials using STS. ✔

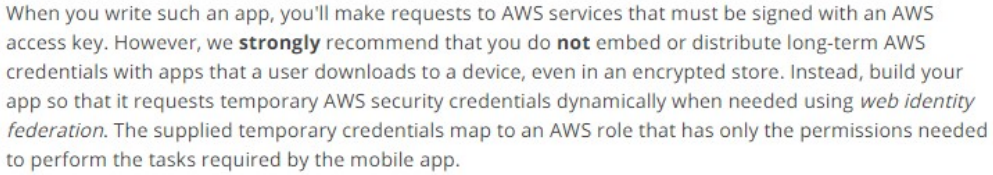
○ **D.** Create an Active Directory server and an AD user for each mobile application user. When the user signs in to the AD sign-on, allow the AD server to federate using SAML 2.0 to IAM and assign a role to the AD user which is the assumed with AssumeRoleWithSAML.

Explanation :

Answer – C

Option A is incorrect because IAM Roles are preferred over IAM Users, because IAM Users have to access the AWS resources using access and secret keys, which is a security concern.
Option B is this is not a feasible configuration.
Option C is CORRECT because it (a) creates an IAM Role with the needed permissions to connect to DynamoDB, (b) it authenticates the users with Web Identity Federation, and (c) the application accesses the DynamoDB with temporary credentials that are given by STS.
Option D is incorrect because the step to create the Active Directory (AD) server and using AD for authenticating is unnecessary and costly.

See the image below for more information on AssumeRoleWithWebIdentity API.


When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we **strongly** recommend that you do **not** embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using *web identity federation*. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app.

For more information on web identity federation please refer to the below link
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html)

Ask our Experts

QUESTION 25 UNATTEMPTED COSTING

In an attempt to cut costs your accounts manager has come to you and tells you that he thinks that if the company starts to use consolidated billing that it will save some money. He also wants the billing set up in such a way that it is relatively simple, and it gives insights into the environment regarding utilization of resources. Which of the following consolidated billing setups would satisfy your account manager's needs?

Choose two answers from the options below

☐ **A.** Use multiple VPC's to break out environments, tag the resources and use a single account. ✔

☐ **B.** Use one master account and no linked accounts.

- [ ] **C.** Use one master account and many member accounts ✔
- [ ] **D.** Use roles for IAM account simplicity across multiple AWS linked accounts.

Explanation :

Answer – A and C
Each organization in AWS Organizations has a *master account* that pays the charges of all the *member accounts*. If you have access to the master account, you can see a combined view of the AWS charges that are incurred by the member accounts.
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html (https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html)

We can have multiple VPC's serving various departments and we can use tags to define them and can have one billing account. The tags associated with the VPC's will distinguish each department or environment.
There are two main considerations in this scenario: (1) Use of Consolidated Billing offered by AWS, and (2) ability to get the insights into the environment regarding the utilization of the resources.
Option A is CORRECT because VPC helps you segregate and organize your resources as per the functionality or domain, thus enabling the account owner to get the insight of the costing of the resources within the logical grouping of the resources. e.g. If an organization has separate VPC for each department - Finance, Development, Sales etc. It will be convenient to get the billing details per department.
Option B is incorrect because if all the resources are created under a single account, it will be difficult for the accounts manager to get insights into the utilization of resources as per the domains or functionality. e.g. Instead of having a separate department such as Finance, Development, Sales etc., if an organization has a single account, it will be tedious to get the details on the billing of each departmental resource.
Option C is CORRECT as having linked account would enable the accounts manager to leverage the Consolidated Billing for multiple AWS accounts. With Consolidated Billing, you can see a combined view of AWS charges incurred by all accounts, as well as get a cost report for each account associated with your payer account.
Option D is incorrect because only IAM Roles will not be sufficient for Consolidated Billing.

For more information on consolidated billing, please refer to the below link
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html (http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html)
You can also have the option of segregating the resources via multiple VPC's and have the billing estimates done via each VPC.
For more information on AWS VPC please refer to the below link
https://aws.amazon.com/vpc/ (https://aws.amazon.com/vpc/)

Ask our Experts

QUESTION 26 UNATTEMPTED SECURITY

The DDoS attacks that happen at the application layer commonly target web applications with lower volumes of traffic compared to infrastructure attacks. To mitigate these types of attacks, you should probably want to include a WAF (Web

Application Firewall) as part of your infrastructure. To inspect all HTTP requests, WAFs sit in-line with your application traffic. Unfortunately, this creates a scenario where WAFs can become a point of failure or bottleneck. To mitigate this problem, you need the ability to run multiple WAFs on demand during traffic spikes. This type of scaling for WAF is done via a “WAF sandwich.” Which of the following statements best describes what a “WAF sandwich" is? Choose the correct answer from the options below

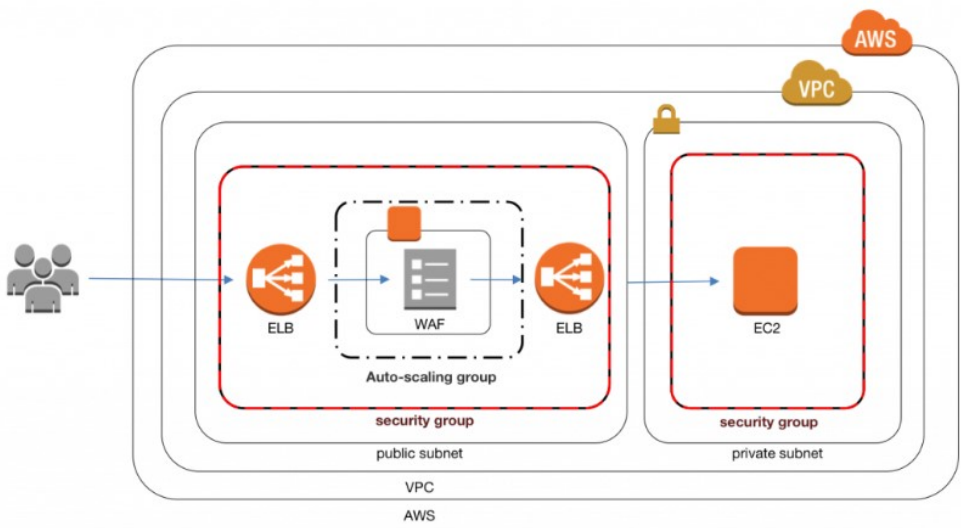
- **A.** The EC2 instance running your WAF software is placed between your private subnets and any NATed connections to the Internet.
- **B.** The EC2 instance running your WAF software is placed between your public subnets and your Internet Gateway.
- **C.** The EC2 instance running your WAF software is placed between your public subnets and your private subnets.
- **D.** The EC2 instance running your WAF software is included in an Auto Scaling group and placed in between two Elastic load balancers. ✔

Explanation :

Answer – D

As shown in the "WAF Sandwich" diagram, the WAF EC2 instances are placed in an auto-scaling group, thus it can scale according to the increase in the incoming traffic load. The ELB on the left of the WAF is a public facing ELB which accepts the incoming traffic and sends to the WAF, which inspects and filters the malicious traffic, and forwards the safe traffic to the ELB on its right side - which is an internal ELB. This ELB then distributes the traffic among the EC2 instances for further processing.

The only correct option is D, because it has the WAF EC2 instance is placed in an autoscaling group and between two ELBs.



For more information on a WAF sandwich please refer to the below link

https://www.cloudaxis.com/2016/11/21/waf-sandwich/ (https://www.cloudaxis.com/2016/11/21/waf-sandwich/)

Ask our Experts

QUESTION 27 UNATTEMPTED COSTING

A company is designing a high availability solution for a customer. This customer requires that their application needs to be able to handle an unexpected amount of load and allow site visitors to read data from a DynamoDB table, which contains the results of an online polling system. At any given time as many as 10,000 requests need to be handled by the application. Given this information, what would be the best and most cost-saving method for architecting and developing this application? Choose the correct answer from the options below

- **A.** Use the JavaScript SDK and build a static HTML page, hosted inside of an Amazon S3 bucket; use CloudFront and Route 53 to serve the website, which uses JavaScript client-side language to communicate with DynamoDB. ✔
- **B.** Create a CloudFront distribution that serves the HTML web page, but send the visitors to an Auto Scaling ELB application pointing to EC2 instances.
- **C.** Deploy an Auto Scaling application with Elastic Load Balancer pointing to EC2 instances that use a server-side SDK to communicate with the DynamoDB table.
- **D.** Create a Lambda script which pulls the most recent DynamoDB polling result and creates a custom HTML page in S3 as per the user request and use CloudFront and Route 53 to serve the static website.

Explanation :

Answer – A

The most important design consideration of this question is to have a highly scalable, cost-saving architecture that provides an application that can communicate with DynamoDB.

Option A is CORRECT because (a) to show the polling results, a static HTML page that is stored in S3 bucket is sufficient as well as cost-effective, (b) CloudFront and Route53 are AWS managed services that are highly available and scalable, and (c) it uses the JavaScript to communicate with DynamoDB.
Option B is incorrect because (a)it will require large number of EC2 instances to handle the load of incoming traffic, and (b) setting up the EC2 instances and ELB is not a cost-effective solution compared to the static web page in S3.
Option C is incorrect because architecting this with ELB and EC2 instances will not be as cost effective as the static HTML page - that communicates with DynamoDB - hosted in S3.
Option D is Incorrect. Lambda uses a default safety throttle for the number of concurrent executions across all functions in a given region per account. Currently, the concurrent execution limit is 1000 and we need to handle ten times the traffic at any point in time. Hence this solution is invalid.

For more information on AWS s3 please refer to the below link
http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html)

Ask our Experts

QUESTION 28 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

You're migrating an existing application to the AWS cloud. The application will be only communicating with the EC2 instances with in the VPC. This application needs to be built with the highest availability architecture available. The application currently relies on hardcoded hostnames for intercommunication between the three tiers. You've migrated the application and configured the multi-tiers using the internal Elastic Load Balancer for serving the traffic. The load balancer hostname is demo-app.us-east-1.elb.amazonaws.com. The current hard-coded hostname in your application used to communicate between your multi-tier application is demolayer.example.com. What is the best method for architecting this setup to have as much high availability as possible? Choose the correct answer from the options below

- **A.** Create an environment variable passed to the EC2 instances using user-data with the ELB hostname, demo-app.us-east-1.elb.amazonaws.com.
- **B.** Create a private resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com ✔
- **C.** Create a public resource record set using Route 53 with a hostname of demolayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com
- **D.** Add a cname record to the existing on-premise DNS server with a value of demo-app.us-east-1.elb.amazonaws.com. Create a public resource record set using Route 53 with a hostname of applayer.example.com and an alias record to demo-app.us-east-1.elb.amazonaws.com.

Explanation :

Answer – B
Since demolayer.example.com is an internal DNS record, the best way is Route 53 to create an internal resource record. One can then point the resource record to the create ELB.
While ordinary Amazon Route 53 resource record sets are standard DNS resource record sets, *alias resource record sets* provide an Amazon Route 53–specific extension to DNS functionality. Instead of an IP address or a domain name, an alias resource record set contains a pointer to a CloudFront distribution, an Elastic Beanstalk environment, an ELB Classic or Application Load Balancer, an Amazon S3 bucket that is configured as a static website, or another Amazon Route 53 resource record set in the same hosted zone.

Option A is incorrect because it does not mention how the mapping between the existing hard-coded host name and the ELB host name.
Option B is CORRECT because it creates an internal ALIAS record set where it defines the mapping between the hard-coded host name and the ELB host name that is to be used.
Option C and D are incorrect because it should create a private record set, not public, since the mapping between the hard-coded host name and ELB host name should be done internally.

For more information on alias and non-alias records please refer to the below link
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html (http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html)

Ask our Experts

QUESTION 29 UNATTEMPTED SECURITY

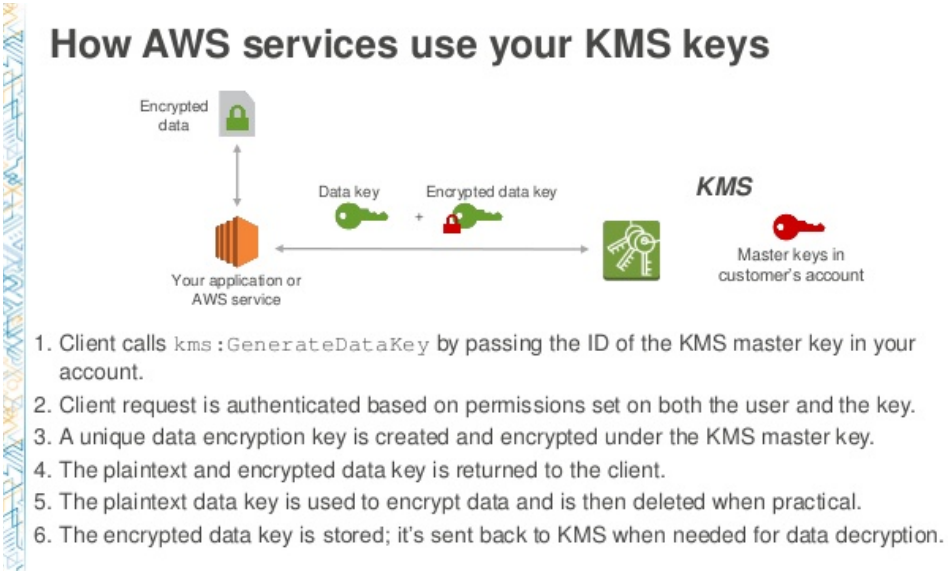
When it comes to KMS, which of the following best describes how the AWS Key Management Service works? Choose the correct answer from the options below

- **A.** AWS KMS supports two kinds of keys — master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The master keys are then used to encrypt and decrypt customer data.
- **B.** AWS KMS supports two kinds of keys — master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The data keys are then used to encrypt and decrypt customer data. ✔
- **C.** AWS KMS supports two kinds of keys — master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The data keys are then used to decrypt the customer data, and the master keys are used to encrypt the customer data.
- **D.** AWS KMS supports two kinds of keys — master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes of data and can also be used to protect data keys. The data keys are then used to encrypt the customer data and the master keys are used to decrypt the customer data.

Explanation :

Answer – B

AWS KMS supports two types of keys - Master Keys and Data Keys. A Data Key is used to encrypt and decrypt the actual data; whereas, the Master Key is used to protect (encrypt and decrypt) the data key as well as some data upto 4Kib. See the image below:



Based on this, option B is CORRECT.

For more information on the AWS KMS Concepts, please refer to the link below:
https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html
(https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html)

Ask our Experts

QUESTION 30 UNATTEMPTED NETWORK DESIGN

A company is building an AWS Cloud Environment for a financial regulatory firm. Part of the requirements is being able to monitor all changes in an environment and all traffic sent to and from the environment. What suggestions would you make to ensure all the requirements for monitoring the financial architecture are satisfied?

Choose the 2 correct answers from the options below

- ☐ **A.** Configure an IPS/IDS in promiscuous mode, which will listen to all packet traffic and API changes.
- ☐ **B.** Configure an IPS/IDS system, such as Palo Alto Networks, using promiscous mode that monitors, filters, and alerts of all potential hazard traffic leaving the VPC.
- ☐ **C.** Configure an IPS/IDS to listen and block all suspected bad traffic coming into and out of the VPC. Configure CloudTrail with CloudWatch Logs to monitor all changes within an environment. ✔
- ☐ **D.** Configure an IPS/IDS system, such as Palo Alto Networks, that monitors, filters, and alerts of all potential hazard traffic sent to and from the VPC. ✔

Explanation :

Answer – C and D

Option A and B both are incorrect because promiscuous mode is not supported in AWS.
Option C is CORRECT because (a) it detects and blocks the malicious traffic coming into and out of VPC, and (b) it also leverages CloudTrail logs and CloudWatch to monitor all the changes in the environment.
option D is CORRECT because it monitors, filters, and alerts about the potentially hazardous traffic leaving from VPC.

Please find the below developer forums thread on the same.
https://forums.aws.amazon.com/thread.jspa?threadID=35683
(https://forums.aws.amazon.com/thread.jspa?threadID=35683)
Please find the below URL to a good slide deck from AWS for getting IDS in place.
https://awsmedia.s3.amazonaws.com/SEC402.pdf
(https://awsmedia.s3.amazonaws.com/SEC402.pdf)

Ask our Experts

QUESTION 31 UNATTEMPTED DEPLOYMENT MANAGEMENT

You have acquired a new contract from a client to move all of his existing infrastructures onto AWS. You notice that he is running some of his applications using multicast, and he needs to keep it running as such when it is migrated to AWS. You discover that multicast is not available on AWS, as you cannot manage multiple subnets on a single interface on AWS and a subnet can only belong to one availability zone. Which of the following would enable you to deploy legacy applications on AWS that require multicast? Choose the correct answer from the options below

- **A.** Provide Elastic Network Interfaces between the subnets.
- **B.** Create a virtual overlay network that runs on the OS level of the instance. ✔
- **C.** All of the answers listed will help in deploying applications that require multicast on AWS.
- **D.** Create all the subnets on a different VPC and use VPC peering between them.

Explanation :

Answer – B

Option A is incorrect because just providing ENIs between the subnets would not resolve the dependency on multicast.
Option B is CORRECT because overlay multicast is a method of building IP level multicast across a network fabric supporting unicast IP routing, such as Amazon Virtual Private Cloud (Amazon VPC).
Option C is incorrect because the only option that will work in this scenario is creating a virtual overlay

network.
Option D is incorrect because VPC peering and multicast are not the same.

For more information on Overlay Multicast in Amazon VPC, please visit the URL below:
https://aws.amazon.com/articles/6234671078671125
(https://aws.amazon.com/articles/6234671078671125)

Ask our Experts

QUESTION 32 UNATTEMPTED COSTING

A company has three consolidated billing accounts; development, staging, and production. The development account has purchased three reserved instances with instance type of m4.large in Availability Zone us-east-1a. However, no instance is running on the development account, but has five m4.large instances running in the staging account which is also in Availability Zone 1a. Who can receive the benefit of the reserved instance pricing? Choose the correct answer from the options below

- **A.** All the instances in all the accounts running the m4.large will receive the pricing even if there is only one reserved instance purchase.
- **B.** No account will receive the reservation pricing because the reservation was purchased on the development account and no instances that match the reservation are running in the development account.
- **C.** The reserved instance pricing will be applied to the instances in the staging account because the staging account is running an instance that matches the reserved instance type. ✔
- **D.** Only the primary account (the consolidated billing primary account) will receive the discounted pricing if the instance is running in the primary billing account.

Explanation :

Answer – C

Option A is incorrect because the benefit of reserved instance pricing will be applicable to any three EC2 instances across all the accounts in the Consolidated Billing group. Since the staging account - which is part of the "account family" - has 5 EC2 instances running, only 3 of those will receive the reserved pricing benefit.
Option B is incorrect because even though there are no EC2 instances running in the development account, the instances running in the staging account will still receive the reservation pricing benefit since it is the part of the Consolidated Billing group.
Option C is CORRECT because the reserved instance pricing be applied to the staging account as it is part of the Consolidated Billing group and only three EC2 instances will be charged with the reserved instance price.
Option D is incorrect because the reserved Consolidated Billing advantage is applied to all the accounts that are linked to the primary account, not just the primary account.

More information on Consolidated Billing Group

Here is how consolidated bills are calculated:

1. A Reserved Instance is a capacity reservation. It is not a virtual machine. It is a commitment by a customer to pay in advance for specific Amazon EC2 or Amazon RDS instance capacity. In return, the customer gets a discounted rate over the cost of an On-Demand instance that is created or deleted in response to application load. From a technical perspective, there is no difference between a Reserved Instance and an On-Demand instance. When a customer launches an instance, AWS checks the account records for Reserved Instance purchases that can be applied to that instance.

2. Consolidated Billing customers have multiple accounts that roll up into a single account that is designated as the payer account. This group of accounts is often called an *account family*. Owners of payer accounts see all usage incurred by the account family. This activity is aggregated to the payer account, and then *allocated* to the linked accounts that generated the charge in proportion to the linked account's usage. In other words, the linked account line items that you see in AWS Cost and Usage report and monthly billing (hourly) reports and on the **Account Activity** page are calculated recursively: The charges are calculated at the payer level and then allocated to linked accounts. Blended rates appear only on linked account line items.

For more information on consolidating billing please visit the below link

- http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html (http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html)
- https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidatedbilling-other.html (https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidatedbilling-other.html)

Ask our Experts

QUESTION 33 UNATTEMPTED DEPLOYMENT MANAGEMENT

A company has developed a Ruby on Rails content management platform. Currently, OpsWorks with several stacks for dev, staging, and production is being used to deploy and manage the application. Now, the company wants to start using Python instead of Ruby. How should the company manage the new deployment such that it should be able to revert back to the old application with Ruby if the new deployment starts adversely impacting the existing customers? Choose the correct answer from the options below

- **A.** Create a new stack that contains the Python application code and manages separate deployments of the application via the secondary stack using the deploy lifecycle action to implement the application code.

- **B.** Create a new stack that contains a new layer with the Python code. Route only a small portion of the production traffic to use the new deployment stack. Once the application is validated, slowly increase the production traffic to the new stack using the Canary Deployment. Revert to the old stack, if the new stack deployment fails or does not work. ✔
- **C.** Create a new stack that contains the Python application code. Route all the traffic to the new stack at once so that all the customers get to access the updated application.
- **D.** Update the existing host instances of the application with the new Python code. This will save the cost of having to maintain two stacks, hence cutting down on the costs.

Explanation :

Answer – B

Option A is incorrect because it mentions how the code would be deployed using the deploy lifecycle event, however it does not mention how the system can revert back to the old application deployment stack if there is any failure.
Option B is CORRECT because it deploys the new stack via the canary deployment method where the new stack is tested only on a small portion production traffic first. If the new deployment has any errors it reverses back to the old deployment stack.
Option C is incorrect even though create the new stack you should always test it a small portion of production traffic with the new stack rather than routing all the production traffic to it.
Option D is incorrect because updating all the production instances at once is risky and it does not give an option to revert back to the old stack in case of any errors.

More information on Canary Deployment
Canary deployments are a pattern for rolling out releases to a subset of users or servers. The idea is to first deploy the change to a small subset of servers, test it, and then roll the change out to the rest of the servers. The canary deployment serves as an early warning indicator with less impact on downtime: if the canary deployment fails, the rest of the servers aren't impacted.

Ask our Experts

QUESTION 34 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your application is having a very high traffic, so you have enabled autoscaling in the multi-availability zone to suffice the needs of your application but you observe that one of the availability zones is not receiving any traffic. What can be wrong here?

- **A.** Autoscaling only works for single availability zone
- **B.** Autoscaling can be enabled for multi AZ only in north Virginia region
- **C.** Availability zone is not added to Elastic load balancer ✔

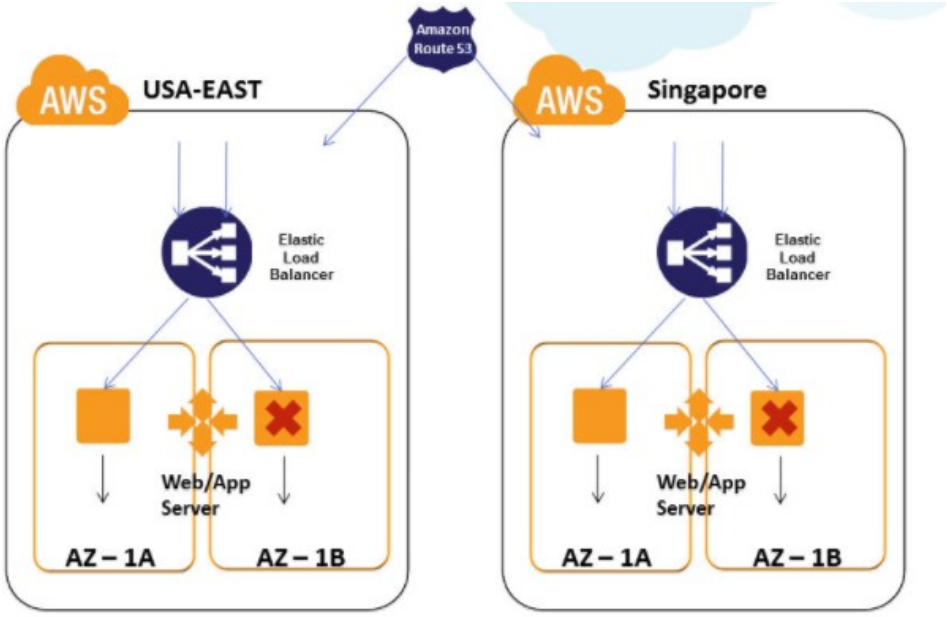
D. Instances need to manually added to availability zone

Explanation :

Answer – C

In order to make sure that all the EC2 instances behind a cross-zone ELB receive the requests, make sure that all the applicable availability zones (AZs) are added to that ELB.

Option A is incorrect because autoscaling can work with multiple AZs.
Option B is incorrect because autoscaling can be enabled for multi AZ in any single region, not just N. Virginia. (see the image below)
Option C is CORRECT because most likely the reason is that the AZ – whose EC2 instances are not receiving requests – is not added to the ELB.
Option D is incorrect because instances need not be added manually to AZ (they should already be there!).



More information on adding AZs to ELB
When you add an Availability Zone to your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. Load balancer nodes accept traffic from clients and forward requests to the healthy registered instances in one or more Availability Zones.
For more information on adding AZ's to ELB, please refer to the below URL
http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-az.html
(http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-az.html)

Ask our Experts

QUESTION 35 UNATTEMPTED SECURITY

A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that will occur on AWS. How can the company meet the auditor's requirements without compromising with the security in the AWS environment?

Choose the correct answer from the options below

- **A.** Create a role that has the required permissions for the auditor.
- **B.** Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
- **C.** The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
- **D.** Enable CloudTrail and specify the S3 bucket for your log file delivery. Create an IAM user who has read only permission to the required AWS resources including the bucket containing CloudTrail logs. ✔

Explanation :

Answer – D

- Option A is incorrect. IAM roles are a secure way to grant permissions to entities that you trust. But the entities should be an IAM user in another account or an User from a corporate directory who use identity federation with SAML. None of these are specified in the question.
- Option B is incorrect because sending the logs via email is not a good architecture.
- Option C is incorrect because granting the auditor access to AWS resources is not AWS's responsibility. It is the AWS user or account owner's responsibility.

AWS CloudTrail is now enabled **by default** for **ALL CUSTOMERS** and will provide visibility into the past seven days of account activity without the need for you to configure a trail in the service to get started. But if you want to access your CloudTrail log files directly or archive your logs for auditing purposes, you can still create a trail and specify the S3 bucket for your log file delivery.

- https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-aws-customers/ (https://aws.amazon.com/blogs/aws/new-amazon-web-services-extends-cloudtrail-to-all-aws-customers/)

More information on AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

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

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

Ask our Experts

QUESTION 36 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

After configuring a whole site CDN on CloudFront you receive the following error: This distribution is not configured to allow the HTTP request method that was used for this request. The distribution supports only cachable requests. What is the most likely cause of this? Choose the correct answer from the options below

- **A.** The CloudFront distribution is configured to the wrong origin
- **B.** Allowed HTTP methods on that specific origin is only accepting GET, HEAD ✔
- **C.** Allowed HTTP methods on that specific origin is only accepting GET, HEAD, OPTIONS
- **D.** Allowed HTTP methods on that specific origin is only accepting GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Explanation :

Answer – B

The AWS documentation also states that "CloudFront caches responses to *GET* and *HEAD* requests" and, optionally, OPTIONS requests. CloudFront **does not cache responses to requests that use the other methods.**

As per AWS documentation,
Allowed HTTP Methods
Specify the HTTP methods that you want CloudFront to process and forward to your origin:

- **GET, HEAD:** You can use CloudFront only to get objects from your origin or to get object headers.
- **GET, HEAD, OPTIONS:** You can use CloudFront only to get objects from your origin, get object headers, or retrieve a list of the options that your origin server supports.
- **GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE:** You can use CloudFront to get, add, update, and delete objects, and to get object headers. In addition, you can perform other POST operations such as submitting data from a web form.

Note
CloudFront caches responses to *GET* and *HEAD* requests and, optionally, *OPTIONS* requests.
CloudFront does not cache responses to requests that use the other methods.

Based on this, Option B seems to be a better choice than C.

For more information please visit:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesAllowedHTTPMethods (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesAllowedHTTPMethods)

When the CloudFront Distribution supports only "cacheable requests", it means that it supports only GET and HEAD HTTP requests (read only). For the HTTP requests such as OPTIONS, PUT, POST, PATCH AND DELETE, the CloudFront will give an error "The distribution supports only cacheable requests".
Hence, option B is the correct answer.
There is a good question posted on StackOverflow which explains what should be done in this situation.
http://stackoverflow.com/questions/31253694/this-distribution-is-not-configured-to-allow-the-http-request (http://stackoverflow.com/questions/31253694/this-distribution-is-not-configured-to-allow-the-http-request)

Ask our Experts

QUESTION 37 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

You're running a financial application on an EC2 instance. Data is stored in the instance is critical and in the event of a failure of an EBS volume, the RTO and RPO are less than 1 minute. How would you architect this application given the RTO and RPO requirements? Choose the correct answer from the options below

- **A.** Mirror the data using RAID 1 configuration, which provides fault tolerance on EBS volumes. ✔
- **B.** Nothing is required since EBS volumes are durability backed up to additional hardware in the same availability zone.
- **C.** Write a script to create automated snapshots of the EBS volumes every minute. In the event of failure have an automated script that detects failure and launches a new volume from the most recent snapshot.
- **D.** Stripe multiple EBS volumes together with RAID 0, which provides fault tolerance on EBS volumes.

Explanation :

Answer – A
To meet the requirement of RTO and RPO less than 1 minute, the best way is to have a configuration where the data is backed up on another EBS volumes. In case of failure, the backup EBS volumes can be used and not data would be lost.
Option A is CORRECT because, as mentioned above, RAID 1 configuration maintains the exact copy of the data (via mirroring) in a backup EBS volume which can be used in case of the failure of the main volume, providing redundancy and fault tolerance. In case of failure, the old EBS volume can quickly be replaced with the backup volume and the RTO and RPO requirement can be met within a minute.
Option B is incorrect because, although each Amazon EBS volume is automatically replicated within its Availability Zone, it is done so to protect it from any component failure from AWS side. It does not withstand any failures at user level. It is user's responsibility to replicate the data that is stored on the EBS volume.
Option C is incorrect because automated snapshots every minute will not meet this RTO and RPO

requirement.
Option D is incorrect because RAID 0 configuration helps improve the performance, but does not provide redundancy or mirroring of the data across disks. As a result of having data striped across all disks, any failure will result in total data loss.

More information on RAID Configurations with EBS volumes:
As per the AWS documentation, it is clearly given to use RAID 1 configuration for fault tolerance of EBS volumes.
With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together.
For more information on RAID configuration, please visit the below URL
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html)

Ask our Experts

QUESTION 38 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

A company is running a MySQL RDS instance inside AWS; however, a new requirement for disaster recovery is keeping a read replica of the production RDS instance in an on-premise data center. What is the securest way of performing this replication? Choose the correct answer from the options below

- **A.** Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.
- **B.** RDS cannot replicate to an on-premise database server. Instead, first configure the RDS instance to replicate to an EC2 instance with core MySQL, and then configure replication over a secure VPN/VPG connection.
- **C.** Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint.
- **D.** Use mysqldump to transfer the database from Amazon RDS instance to external MySQL database. Create an IPSec VPN connection using VPN/VGW through Virtual Private Cloud service. ✔

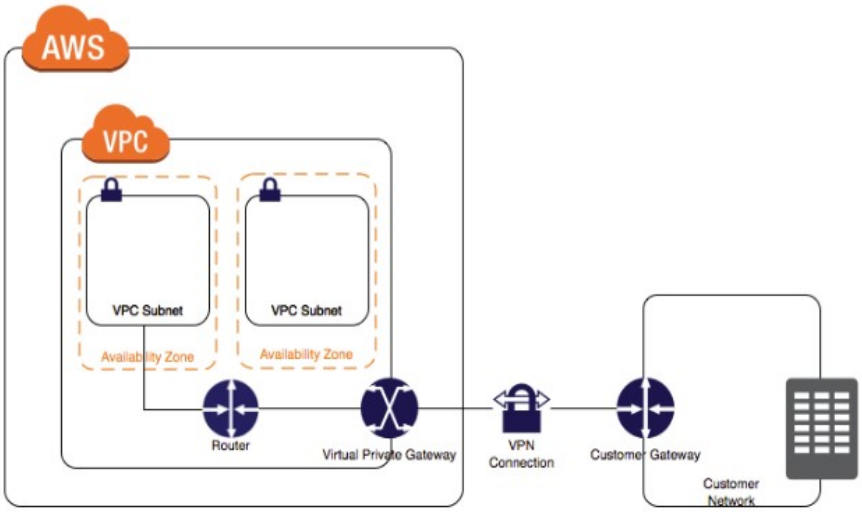
Explanation :

Answer – D

- Option A is incorrect because SSL endpoint cannot be used here as it is used for securely accessing the database.
- Option B is incorrect because replicating via EC2 instances is very time consuming and very expensive cost-wise.
- Option C is incorrect because Data Pipeline is for batch jobs and not suitable for this scenario.

- Option D is CORRECT because it is feasible to setup the secure IPSec VPN connection between the on premise server and AWS VPC using the VPN/Gateways.

See the image below:



For more information on VPN connections , please visit the below URL:

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

Note:
AWS docs state that,
Configure an egress rule for the external instance to operate as a Read Replica during the export. The egress rule will allow the MySQL Read Replica to connect to the MySQL DB instance during replication. Specify an egress rule that allows TCP connections to the port and IP address of the source Amazon RDS MySQL DB instance.

Please refer the following link for more information.

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MySQL.Procedural.Exporting.NonRDSRepl.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MySQL.Procedural.Exporting.NonRDSRepl.html)

Also as per AWS docs
we can set up replication between an Amazon RDS MySQL or MariaDB DB instance and a MySQL or MariaDB instance that is external to Amazon RDS.

Please find the link for more details:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MySQL.Procedural.Importing.External.Repl.html (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MySQL.Procedural.Importing.External.Repl.html)

Out of the options provided Choice D seems to be safest one security wise as it allows secure connections over the IPSec VPN tunnel.

Ask our Experts

QUESTION 39 UNATTEMPTED SECURITY

You are setting up a video streaming service with the main components of the set up being S3, CloudFront, and Transcoder. Your video content will be stored on AWS S3 and it should only be viewed by the subscribers who have paid for the service. Your first job is to upload 10 videos to S3 and make sure they are secure before you even begin to start thinking of streaming the videos. The 10 videos have just finished uploading to S3, so you now need to secure them with encryption at rest. Which of the following would be the best way to do this? Choose the correct answer from the options below:

- **A.** Use AWS CloudHSM appliance with both physical and logical tamper detection and response mechanisms that trigger zeroization of the appliance.
- **B.** Encrypt your data using AES-256. After the object is encrypted, the encryption key you used needs to be stored on AWS CloudFront so that only authenticated users can stream the videos.
- **C.** Set an API flag, or check a box in the AWS Management Console, to have data encrypted in Amazon S3. Create IAM Users to access the videos from S3.
- **D.** Use KMS to encrypt source data and decrypt resulting output. Also, use Origin Access Identity on your CloudFront distribution, so the content is only able to be served via CloudFront, not S3 URLs. ✔

Explanation :

Answer – D

There are two main considerations in this scenario: (1) the data in S3 should be encrypted "at rest", and (2) only the authenticated users should be able to stream the video.

Option A is incorrect because because AWS CloudHSM is used for generating the user's own encryption keys on the AWS Cloud. It does not encrypt any data on S3 at rest.
Option B is incorrect because, even though it encrypts the data at rest, storing the keys in the CloudFront for private access to the authenticated users is an invalid solution.
Option C is incorrect because there is no checkbox in AWS Console to apply the encryption on S3 data. You need to apply the appropriate policy to the bucket if you require server-side encryption for all objects in it.
Option D is CORRECT because, (a) it uses KMS for encrypting and decrypting the data, and (b) it ensures that only the authenticated users will have access to the videos by using the Origin Access Identity (OAI) on the CloudFront distribution and disabling the access via S3 URLs.

Below is a good link for how to use either SSE S3 or KMS encryption
https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#more-1038 (https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#more-1038)
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html)

Ask our Experts

QUESTION 40 UNATTEMPTED DEPLOYMENT MANAGEMENT

You currently have 9 EC2 instances running in a Placement Group. All these nine instances were initially launched at the same time and seemed to be performing as expected. You decide that you need to add two new instances to the group; however, when you attempt to do this you receive a 'capacity error.' Which of the following actions will most likely fix this problem? Choose the correct answer from the options below

- **A.** Make a new Placement Group and launch the new instances in the new group. Make sure the Placement Groups are in the same subnet.
- **B.** Stop and restart the instances in the Placement Group and then try the launch again. ✔
- **C.** Request a capacity increase from AWS as you are initially limited to 10 instances per Placement Group.
- **D.** Make sure all the instances are the same size and then try the launch again.

Explanation :

Answer – B

Option A is incorrect because to benefit from the enhanced networking, all the instances should be in the same Placement Group. Launching the new ones in a new Placement Group will not work in this case.

Option B is CORRECT because the most likely reason for the "Capacity Error" is that the underlying hardware may not have the capacity to launch any additional instances on it. If the instances are stopped and restarted, AWS may move the instances to a hardware that has capacity for all the requested instances.

Option C is incorrect because there is no such limit on the number of instances in a Placement Group (however, you can not exceed your EC2 instance limit allocated to your account per region).

Option D is incorrect because the capacity error is not related to the instance size and just ensuring that the instances are of same size will not resolve the capacity error.

More information on Cluster Placement Group

If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Restarting the instances may migrate them to hardware that has the capacity for all the requested instances.

Cluster Placement Groups

A cluster placement group is a logical grouping of instances within a single Availability Zone. A placement group can span peered VPCs in the same region.

Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both, and if the majority of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking. For more information, see Enhanced Networking.
We recommend that you launch the number of instances that you need in the placement group in a single launch request and that you use the same instance type for all instances in the placement group. If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error.
If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance.
If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Restarting the instances may migrate them to hardware that has capacity for all the requested instances.

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

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html)

Note:
In this scenario we are discussing about the insufficient capacity error happening with in a placement group.
As per AWS docs,
"If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Restarting the instances may migrate them to hardware that has capacity for all the requested instances."
In our scenario we already have 9 EC2 instances running on a placement group and when we tried to add 2 more to the group we have encountered this error. So if we stop and restart all the instances will help to resolve this issue as the restarting instances will migrate to a new hardware which will have the capacity for all the instances.

For more information please refer:

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

Ask our Experts

QUESTION 41 UNATTEMPTED DEPLOYMENT MANAGEMENT

A company has two batch processing applications that consume financial data about the day's stock transactions. Each transaction needs to be stored durably and guarantee that a record of each application is delivered so the audit and billing batch processing applications can process the data. However, the two applications run separately and several hours apart and need access to the same transaction

information in a serial order. After reviewing the transaction information for the day, the information no longer needs to be stored. What is the best way to architect this application? Choose the correct answer from the options below

- **A.** Use SQS for storing the transaction messages. When the billing batch process consumes each message, have the application create an identical message and place it in a different SQS for the audit application to use several hours later.
- **B.** Use SQS for storing the transaction messages; when the billing batch process performs first and consumes the message, write the code in a way that does not remove the message after consumed, so it is available for the audit application several hours later. The audit application can consume the SQS message and remove it from the queue when completed.
- **C.** Store the transaction information in a DynamoDB table. The billing application can read the rows while the audit application will read the rows them remove the data.
- **D.** Use Kinesis to store the transaction information. The billing application will consume data from the stream, the audit application can consume the same data several hours later. ✔

Explanation :

Answer – D

The main architectural considerations in this scenario are: (1) each transaction needs to be stored durably (no loss of any transaction), (2) they should be processed in serial order, (3) guaranteed delivery of each record to the audit and billing batch processing, and (4) the processing of the record by two application is done with a time gap of several hours.
Based on the considerations above, it seems that we must use Amazon Kinesis Data Streams which enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).

Option A is incorrect because (a) the onus of ensuring that each message is copied to the audit queue is on the application, and (b) this option is not fail-proof. i.e. If the application fails to copy the message between the queue, there is no logic to put the message back to the billing queue.
Option B is incorrect because, even though it uses SQS, there is an overhead of ensuring that the message is put back into the same queue. Also, there is a possibility of processing the same record (message) multiple time by the instances processing it (there is no way to know if the record has been already processed).
Option C is incorrect because it adds the overhead of delivery guarantee on the application itself. Also, the use of DynamoDB in this scenario is not a cost effective solution.
Option D is CORRECT because Amazon Kinesis is best suited for applocations which needs to process large real-time transactional records and have the ability to consume records in the same order a few hours later. For example, you have a billing application and an audit application that runs a few hours behind the billing application. Because Amazon Kinesis Data Streams stores data for up to 7 days, you can run the audit application up to 7 days behind the billing application.

More information on when Amazon Kinesis Data Streams and Amazon SQS should be used:
AWS recommends Amazon Kinesis Data Streams for use cases with requirements that are similar to the following:

- Routing related records to the same record processor (as in streaming MapReduce). For example, counting and aggregation are simpler when all records for a given key are routed to the same record processor.
- Ordering of records. For example, you want to transfer log data from the application host to the processing/archival host while maintaining the order of log statements.
- Ability for multiple applications to consume the same stream concurrently. For example, you have one application that updates a real-time dashboard and another that archives data to Amazon Redshift. You want both applications to consume data from the same stream concurrently and independently.
- Ability to consume records in the same order a few hours later. For example, you have a billing application and an audit application that runs a few hours behind the billing application. Because Amazon Kinesis Data Streams stores data for up to 7 days, you can run the audit application up to 7 days behind the billing application.

AWS recommends Amazon SQS for use cases with requirements that are similar to the following:

- Messaging semantics (such as message-level ack/fail) and visibility timeout. For example, you have a queue of work items and want to track the successful completion of each item independently. Amazon SQS tracks the ack/fail, so the application does not have to maintain a persistent checkpoint/cursor. Amazon SQS will delete acked messages and redeliver failed messages after a configured visibility timeout.
- Individual message delay. For example, you have a job queue and need to schedule individual jobs with a delay. With Amazon SQS, you can configure individual messages to have a delay of up to 15 minutes.
- Dynamically increasing concurrency/throughput at read time. For example, you have a work queue and want to add more readers until the backlog is cleared. With Amazon Kinesis Data Streams, you can scale up to a sufficient number of shards (note, however, that you'll need to provision enough shards ahead of time).
- Leveraging Amazon SQS's ability to scale transparently. For example, you buffer requests and the load changes as a result of occasional load spikes or the natural growth of your business. Because each buffered request can be processed independently, Amazon SQS can scale transparently to handle the load without any provisioning instructions from you.

https://aws.amazon.com/kinesis/data-streams/faqs/ (https://aws.amazon.com/kinesis/data-streams/faqs/)

Ask our Experts

QUESTION 42 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

A company is considering integrating their on-premises resources with AWS in a hybrid architecture. Their goal is to run the customer-facing data collection processes in AWS. They have to transfer huge volume of data from EC2 instances

running in an AWS VPC to their on-premises environment daily. This high data transfer cost is currently threatening to derail the project. What could you do to help reduce the overall cost of data transfer out of AWS?

- **A.** Provision a VPN connection between the on-premise data center and the AWS region using the VPN section of a VPC.
- **B.** Suggest provisioning a Direct Connect connection between the on-premise data center and the AWS region. ✔
- **C.** Suggest using AWS import/export to transfer the TBs of data while synchronizing the new data as it arrives.
- **D.** Suggest leaving the data required for the application on-premise and use a VPN to query the on-premise database data from EC2 when required.

Explanation :

Answer – B

In this question, the customer wants to transfer large amount of data to VPC from the on-premises data center. The main architectural considerations are (1) the cost should be low, and (2) the data being transferred is new data every time.

Option A is incorrect because, although setting up a VPN is a cost effective solution, it may not have sufficient bandwidth for the data being trasferred, especially since the data is new every time. Also,the data will be transferred over the internet. So, the new data adds to the unpredictability of the performance that the VPN connection would yield. So, the VPN connection may stay much longer than expected adding to the overall cost.
Option B is CORRECT because (a) since it is a dedicated connection from on-premises data center to AWS, it takes out the unpredictable nature of the internet out of the equation, and (2) due to the high bandwidth availability, Direct Connect would most probably transfer the large amount of data quickly compared to VPN connection. Hence, it may well save the cost for the customer.
Option C is incorrect because AWS Import/Export is not an ideal option since the data being transferred is new every time, since Import/Export is preferred mainly for first time data migration and using VPN/Direct Connect later on.
Option D is incorrect because it is the requirement that the data must be transferred to AWS, hence ruling out the option of leaving the data on-premise.

For more information on AWS direct connect, just browse to the below URL
https://aws.amazon.com/directconnect/ (https://aws.amazon.com/directconnect/)

Note: While I agree that the Direct Connect is costly, but compared to other options given, it is certainly the most viable. With the dedicated network connectivity and higher bandwidth, the data transfer would get done quicker compared to over the internet. With Direct Connect, the initial setup cost would be more. But in the long run, it would be the most suitable solution even with regards to keeping the cost low.

Ask our Experts

QUESTION 43 UNATTEMPTED SECURITY

An application has multiple components. The single application and all the components are hosted on a single EC2 instance (without an ELB) in a VPC. You have been told that this needs to be set up with two separate SSLs for each component. Which of the following would best achieve the setting up of the two separate SSLs while using still only using one EC2 instance? Choose the correct answer from the options below

- **A.** Create an EC2 instance which has multiple network interfaces with multiple elastic IP addresses. ✔
- **B.** Create an EC2 instance which has both an ACL and the security group attached to it and have separate rules for each IP address.
- **C.** Create an EC2 instance which has multiple subnets attached to it and each will have a separate IP address.
- **D.** Create an EC2 instance with a NAT address.

Explanation :

Answer – A

It can be useful to assign multiple IP addresses to an instance in your VPC to do the following:

(1) Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address.
(2) Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface.
(3) Redirect internal traffic to a standby instance in case your instance fails, by reassigning the secondary IP address to the standby instance.

Option A is CORRECT because, as mentioned above, if you have multiple elastic network interfaces (ENIs) attached to the EC2 instance, each network IP can have a component running with a separate SSL certificate.
Option B is incorrect because having separate rules in security group as well as NACL does not mean that the instance supports multiple SSLs.
Option C is incorrect because an EC2 instance cannot have multiple subnets.
Option D is incorrect because NAT address is not related to supporting multiple SSLs.

For more information on Multiple IP Addresses, please refer to the link below:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html)

Ask our Experts

QUESTION 44 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

You are working as a consultant for a company designing a new hybrid architecture to manage part of their application infrastructure in the cloud and on-premise. As part of the infrastructure, they need to consistently transfer high amounts of data. They require a low latency and high consistency traffic to AWS. The company is looking to keep costs as low possible and is willing to accept slow traffic in the event of primary failure. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

- **A.** Provision a Direct Connect connection to an AWS region using a Direct Connect partner. Provision a VPN connection as a backup in the event of Direct Connect connection failure. ✔
- **B.** Create a dual VPN tunnel for private connectivity, which increases network consistency and reduces latency. The dual tunnel provides a backup VPN in the case of primary failover.
- **C.** Provision a Direct Connect connection which has automatic failover and backup built into the service.
- **D.** Provision a Direct Connect connection to an AWS region using a Direct Connect provider. Provision a secondary Direct Connect connection as a failover.

Explanation :

Answer – A

AWS Direct Connect makes it easy to establish a dedicated network connection from your on-premises data center to AWS. i.e. You can establish private connectivity between AWS and the on-premises data center, which helps to reduce the overall network cost, increase bandwidth throughput, and provide more consistent network experience than the internet based connection.
A VPN connection is a low-cost, an appliance based access to the AWS resources that is given to the on-premises resources via gateways over the internet. Compared to AWS Direct Connect, the VPN connection may experience slow connection speed and limited bandwidth due to unpredictability of the internet.
Since cost is a factor for the backup and the company does not mind the reduced traffic, the backup option can a VPN connection instead of another direct connect solution.

Option A is CORRECT because it sets up a Direct Connect as the primary connection which provides consistent bandwidth for transferring high amounts of data, and in case of failure, sets up a VPN which is a low-cost solution.
Option B is incorrect because VPN (although set up as dual) does not provide low latency connection as it still has network unpredictability, and consistency as the Direct Connect would do.
Option C is incorrect because there is no automatic failover or redundancy in Direct Connect.
Option D is incorrect because setting up two Direct Connect connections would be costly.

For more information on AWS direct connect, just browse to the below URL
https://aws.amazon.com/directconnect/ (https://aws.amazon.com/directconnect/)

Ask our Experts

QUESTION 45 UNATTEMPTED SECURITY

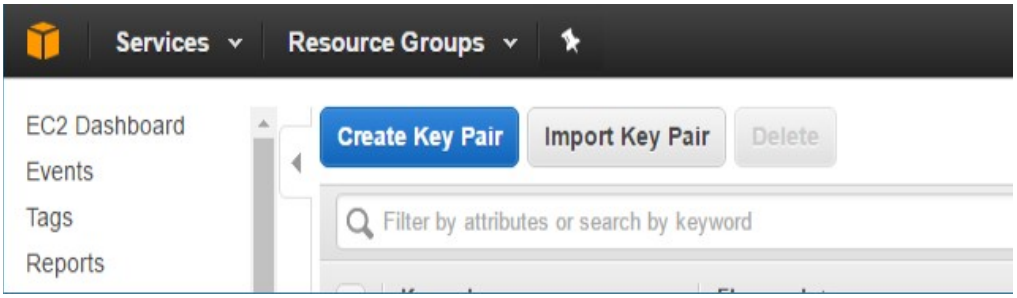
You have a massive social networking application which is already deployed on N.Virginia region with around 100 EC2 instances, you want to deploy your application to multiple regions for better availability. You don't want to handle multiple key pairs and want to reuse existing key pairs for N.Virginia region. How will you accomplish this?

- A. Key pair is not a region level concept, all the keys are available globally
- B. Use copy key command line API to transfer key to different regions
- C. Using import key-pair feature using AWS web console ✔
- D. Copy AMI of your EC2 machine between regions and start an instance from that AMI

Explanation :

Answer - C

Key pairs across regions is not possible. In order to use key pairs across regions you need to import the key pairs in the respective regions.
You need to go the respective region and from the EC2 dashboard , click on Import Key pair and choose the relevant key pair.



Option A is incorrect because key pair is region specific – not global.
Option B is incorrect because keys cannot be copied across different regions, they need to be imported.
Option C is CORRECT because import key pair functionality enables migrating an EC2 instance from one region to another and use the same PEM key.
Option D is incorrect because PEM keys cannot be copied to another region as part of the AMI.

For more information on bringing your own key pair, please refer to the below URL
https://aws.amazon.com/blogs/aws/new-amazon-ec2-feature-bring-your-own-keypair/
(https://aws.amazon.com/blogs/aws/new-amazon-ec2-feature-bring-your-own-keypair/)

Ask our Experts

QUESTION 46 UNATTEMPTED SECURITY

A third party auditor is being brought in to review security processes and configurations for all of a company's AWS accounts. Currently, the company does not use any on-premise identity provider. Instead, they rely on IAM accounts in each of their AWS accounts. The auditor needs read-only access to all AWS resources for each AWS account.Given the requirements, what is the best security method for architecting access for the security auditor? Choose the correct answer from the options below

- **A.** Create an IAM user for each AWS account with read-only permission policies for the auditor, and disable each account when the audit is complete.
- **B.** Configure an on-premise AD server and enable SAML and identify federation for single sign-on to each AWS account.
- **C.** Create an IAM role with read-only permissions to all AWS services in each AWS account. Create one auditor IAM account and add a permissions policy that allows the auditor to assume the ARN role for each AWS account that has an assigned role. ✔
- **D.** Create a custom identity broker application that allows the auditor to use existing Amazon credentials to log into the AWS environments.

Explanation :

Answer – C

Option A is incorrect because creating an IAM User for each AWS account is an overhead and less preferred way compared to creating IAM Role.
Option B is incorrect because the scenario says that the company does not have any on-premises identity provider.
Option C is CORRECT because it creates an IAM Role which has all the necessary permission policies attached to it which allows the auditor to assume the appropriate role while accessing the resources.
Option D is incorrect because using the IAM Role that has the required permissions is the preferred and more secure way of accessing the AWS resources than using the Amazon credentials. Also, this option does not use any Security Token Service that gives temporary credentials to login. Hence this is a less secure way of accessing the AWS resources.

For more information on IAM roles please refer to the below URL
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
(http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

Ask our Experts

QUESTION 47 UNATTEMPTED SECURITY

An auditor needs access to logs that record all the API events on AWS. The auditor only needs read-only access to the log files and does not need access to each AWS account. The company has multiple AWS accounts, and the auditor needs access to all the logs for all the accounts. What is the best way to configure access for the auditor to view event logs from all accounts? Choose the correct answer from the options below

- **A.** Configure the CloudTrail service in each AWS account, and make the logs delivered to an AWS bucket on each account, while granting the auditor permissions to the bucket via roles in the secondary accounts and a single primary IAM account that can assume a read-only role in the secondary AWS accounts.
- **B.** Configure the CloudTrail service in the primary AWS account and configure consolidated billing for all the secondary accounts. Then grant the auditor access to the S3 bucket that receives the CloudTrail log files.
- **C.** Configure the CloudTrail service in each AWS account and enable consolidated logging inside of CloudTrail.
- **D.** Configure the CloudTrail service in each AWS account and have the logs delivered to a single AWS bucket named "seclog" in a separate account created specifically for storing logs. Provide the auditor to access only "seclog" in that separate account. ✔

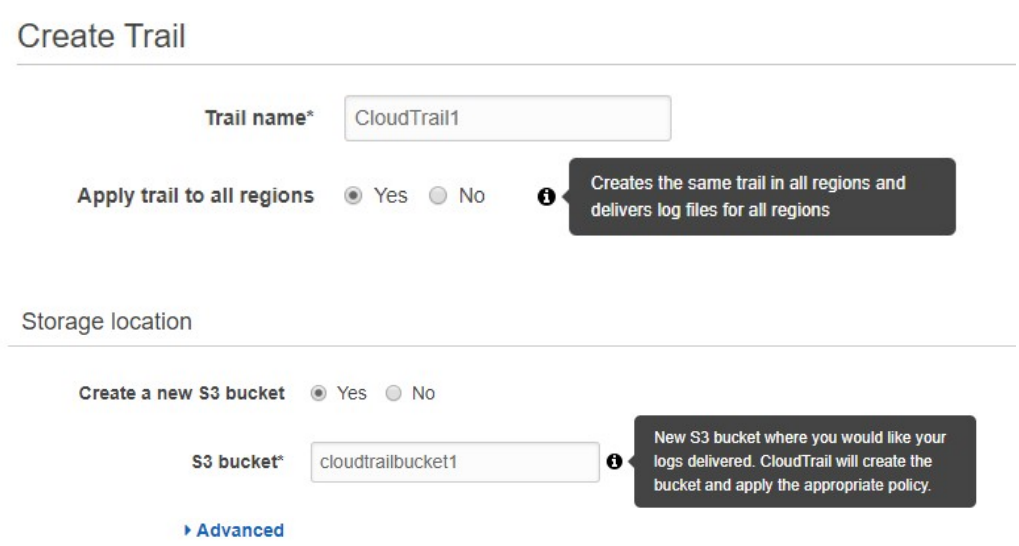
Explanation :

Answer – D

You can have CloudTrail deliver log files from multiple AWS accounts into a single Amazon S3 bucket. For example, you have four AWS accounts with account IDs 111111111111, 222222222222, 333333333333, and 444444444444, and you want to configure CloudTrail to deliver log files from all four of these accounts to a bucket belonging to account 111111111111. To accomplish this, complete the following steps in order:

1. Turn on CloudTrail in the account where the destination bucket will belong (111111111111 in this example). Do not turn on CloudTrail in any other accounts yet.
2. Update the bucket policy on your destination bucket to grant cross-account permissions to CloudTrail.
3. Turn on CloudTrail in the other accounts you want (222222222222, 333333333333, and 444444444444 in this example). Configure CloudTrail in these accounts to use the same bucket belonging to the account that you specified in step 1 (111111111111 in this example).

The AWS CloudTrail service provides with an option to deliver the log files for all the regions in a single S3 bucket. This feature is very useful when you need to access the logs related to all the resources in multiple regions for all the AWS accounts via single S3 bucket. Please see the images below:



Option A is incorrect because delivering the logs in multiple buckets is an unnecessary overhead. Instead, you can have CloudTrail deliver the logs to a single S3 bucket.
Option B is incorrect because consolidated billing will not help the auditor to get the records of all the API events in AWS.
Option C is incorrect because there is no consolidated logging feature in AWS CloudTrail.
Option D is CORRECT because it it delivers the logs pertaining to different AWS accounts to a single S3 bucket in the primary account and grants the auditor the access to it.

More information on this topic regarding CloudTrail:
You can have CloudTrail deliver log files from multiple AWS accounts into a single Amazon S3 bucket. For example, if you have four AWS accounts with account IDs A, B, C, and D, and you can configure CloudTrail to deliver log files from all four of these accounts to a bucket belonging to account A. See the link below:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html)

Ask our Experts

QUESTION 48 UNATTEMPTED DEPLOYMENT MANAGEMENT

An employee keeps terminating EC2 instances on the production environment. You've determined the best way to ensure this doesn't happen to add an extra layer of defense against terminating the instances. What is the best method to ensure that the employee does not terminate the production instances?

Choose the 2 correct answers from the options below

- [ ] **A.** Tag the instance with a production-identifying tag and add resource-level permissions to the employee user with an explicit deny on the terminate API call to instances with the production tag. ✔
- [ ] **B.** Tag the instance with a production-identifying tag and modify the employees group to allow only start, stop, and reboot API calls and not the terminate instance call. ✔
- [ ] **C.** Modify the IAM policy on the user to require MFA before deleting EC2 instances and disable MFA access to the employee
- [ ] **D.** Modify the IAM policy on the user to require MFA before deleting EC2 instances

Explanation :

Answer – A and B

To stop the users from manipulating any AWS resources, you can either create the applicable (allow/deny) resource level permissions and apply them to those users, or create an individual or group policy which explicitly denies the action on that resource and apply it to the individual user or the group.

Option A is CORRECT because it (a) identifies the instances with proper tag, and (b) creates a resource level permission and explicitly denies the user the terminate option.
Option B is CORRECT because it (a) identifies the instances with proper tag, and (b) creates a policy with explicit deny of terminating the instances and applies that policy to the group which contains the employees (who are not supposed to have the access to terminate the instances).
Option C and D are incorrect because MFA is an additional layer of security given to the users for logging into AWS and accessing the resources. However, either enabling or disabling MFA cannot prevent the users from performing resource level actions.

More information on Tags
Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define.
For more information on tagging AWS resources please refer to the below URL
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html)

Ask our Experts

QUESTION 49 UNATTEMPTED COSTING

A company is managing a customer's application which currently includes a three-tier application configuration. The first tier manages the web instances and is configured in a public subnet. The second layer is the application layer. As part of the application code, the application instances upload large amounts of data to Amazon

S3. Currently, the private subnets that the application instances are running on have a route to a single NAT t2.micro NAT instance. The application, during peak loads, becomes slow and customer uploads from the application to S3 are not completing and taking a long time. Which steps might you take to solve the issue using the most cost-efficient method? Choose the correct answer from the options below

- **A.** Configure Auto Scaling for the NAT instance in order to handle increase in load
- **B.** Create a VPC S3 endpoint ✔
- **C.** Increase the NAT instance size; network throughput increases with an increase in instance size
- **D.** Launch an additional NAT instance in another subnet and replace one of the routes in a subnet to the new instance

Explanation :

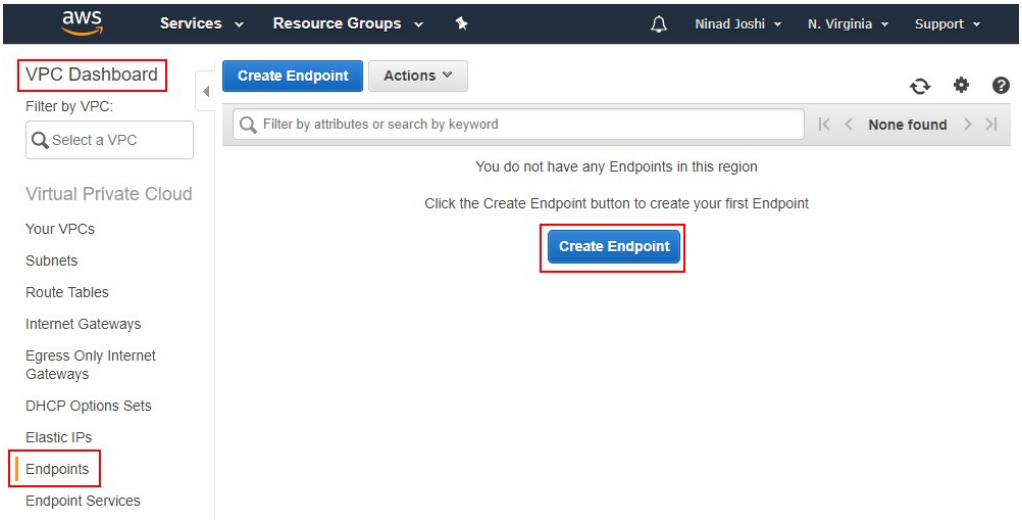
Answer – B

In this scenario, the NAT instance is the bottleneck, which during the peak loads, becomes slow. The possible solutions are either scale up or scale out the NAT instance, or setup S3 as the endpoint of the VPC, so that the VPC can privately and securely connect to the S3 buckets. See the images below for setting up the S3 as VPC Endpoint:

New VPC Endpoint for S3

Today we are simplifying access to S3 resources from within a VPC by introducing the concept of a VPC Endpoint. These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.

EC2 instances running in private subnets of a VPC can now have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.



Option A is incorrect because even though placing NAT instance in auto scale would handle the increase in load, addition of the NAT instances would not be as cost-efficient as creating an S3 endpoint.

Option B is CORRECT because with S3 Endpoint, the VPC can privately and securely connect to the S3 buckets. No additional infrastructure provisioning such as NAT or Gateway is needed, hence saving the cost.
Option C is incorrect because increasing in NAT instance size would add to the cost.
Option D is incorrect because provisioning additional NAT instances would add to the cost.

For more information on VPC endpoints please refer to the below URL:
https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/
(https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/)
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html
(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html)

Ask our Experts

QUESTION 50 UNATTEMPTED SECURITY

A company has many employees who need to run internal applications that access the company's AWS resources. These employees already have user credentials in the company's current identity authentication system, which does not support SAML 2.0. The company does not want to create a separate IAM user for each company employee. How should the SSO setup be designed?

Choose the 2 correct answers from the options below

- ☐ **A.** Create an IAM user to share based off of employee roles in the company.
- ☐ **B.** Create a custom identity broker application which authenticates the employees using the existing system, uses the GetFederationToken API call and passes a permission policy to gain temporary access credentials from STS. ✔
- ☐ **C.** Create a custom identity broker application which authenticates employees using the existing system and uses the AssumeRole API call to gain temporary, role-based access to AWS. ✔
- ☐ **D.** Configure an AD server which synchronizes from the company's current Identity Provide and configures SAML-based single sign-on which will then use the AssumeRoleWithSAML API calls to generate credentials for the employees.

Explanation :

Answers – B and C

Option A is incorrect because creating IAM users is not a best practice and not recommended.
Option B is CORRECT because, (a) it creates custom identity broker application for authenticating the users using their existing credentials, (b) it gets temporary access credentials using STS, and (3) it uses federated access for accessing the AWS resources.
Option C is CORRECT because (a) it creates custom identity broker application for authenticating the users using their existing credentials, and (b) it uses AssumeRole API for accessing the resources using temporary role.

Option D is incorrect because AssumeRoleWithSAML works only with SAML complaint identity providers and the given scenario does not support SAML 2.0.

More information on AssumeRole and GetFederatedToken:
Assume Role - Returns a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) that you can use to access AWS resources that you might not normally have access to. Typically, you use AssumeRole for cross-account access or federation.
For more information , please visit the below URL
http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html
(http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html)
GetFederationToken - Returns a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for a federated user. A typical use is in a proxy application that gets temporary security credentials on behalf of distributed applications inside a corporate network
For more information , please visit the below URL:
http://docs.aws.amazon.com/STS/latest/APIReference/API_GetFederationToken.html
(http://docs.aws.amazon.com/STS/latest/APIReference/API_GetFederationToken.html)

Ask our Experts

QUESTION 51 UNATTEMPTED DATA STORAGE

You have created a mobile application that serves data stored in an Amazon DynamoDB table. Your primary concern is scalability of the application and being able to handle millions of visitors and data requests. As part of your application, the customer needs access to the data located in the DynamoDB table. Given the application requirements, what would be the best method to design the application? Choose the correct answer from the options below

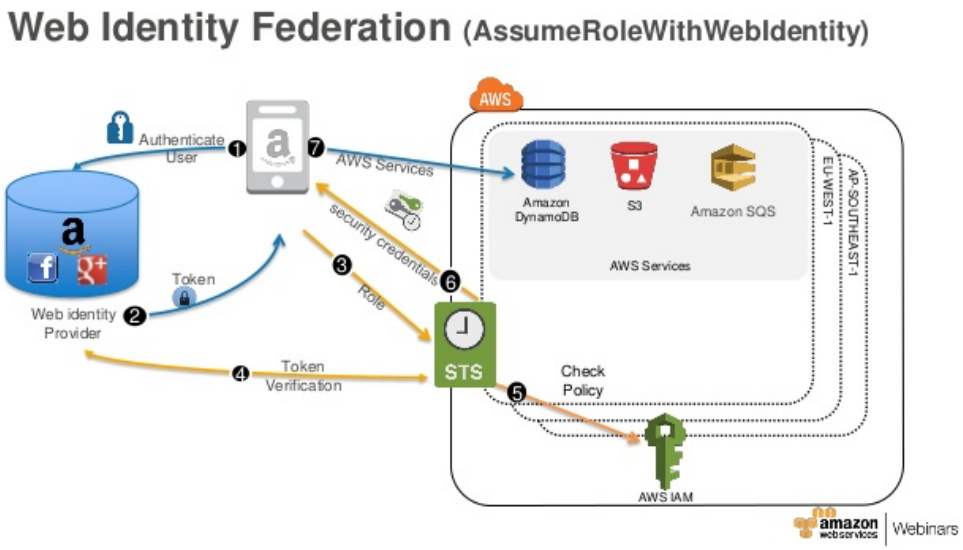
- **A.** Configure an on-premise AD server utilizing SAML 2.0 to manage the application users inside the on-premise AD server and write code that authenticates against the LD serves. Grant a role assigned to the STS token to allow the end-user to access the required data in the DynamoDB table.
- **B.** Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWith API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket.
- **C.** Let the users sign into the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in a server-side language using the AWS SDK and host the application in an S3 bucket for scalability.

O **D.** Let the users sign in to the app using a third party identity provider such as Amazon, Google, or Facebook. Use the AssumeRoleWithWebIdentity API call to assume the role containing the proper permissions to communicate with the DynamoDB table. Write the application in JavaScript and host the JavaScript interface in an S3 bucket. ✔

Explanation :

Answer – D

The AssumeRolewithWebIdentity returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider. Out of option C and D, Option C is invalid because S3 is used to host static websites and not server side language websites.



For more information on AssumeRolewithWebIdentity, please visit the below URL http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html (http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html)

Ask our Experts

QUESTION 52 UNATTEMPTED NETWORK DESIGN

Which of the following is NOT a way to minimize the attack surface area as a DDOS minimization strategy in AWS? Choose the correct answer from the options below

O **A.** Configure services such as Elastic Load Balancing and Auto Scaling to automatically scale. ✔

- B. Reduce the number of necessary Internet entry points.
- C. Separate end user traffic from management traffic.
- D. Eliminate non-critical Internet entry points.

Explanation :

Answer – A
Some important consideration when architecting on AWS is to limit the opportunities that an attacker may have to target your application. For example, if you do not expect an end user to directly interact with certain resources you will want to make sure that those resources are not accessible from the Internet. Similarly, if you do not expect end-users or external applications to communicate with your application on certain ports or protocols, you will want to make sure that traffic is not accepted. This concept is known as attack surface reduction.
Option A is CORRECT because it is used for mitigating the DDoS attack where the system scales to absorb the application layer traffic in order to keep it responsive.
Option B, C and D are incorrect as they all are used for reducing the DDoS attack surface.
For more information on DDoS attacks in AWS, please visit the below URL
https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf
(https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf)

Ask our Experts

QUESTION 53 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

A customer has established an AWS Direct Connect connection to AWS. The link is up and routes are being advertised from the customer's end, however the customer is unable to connect from EC2 instances inside its VPC to servers residing in its data center.

Which of the following options provide a viable solution to remedy this situation? (Choose 2 answers).

- A. Add a route to the route table with an IPsec VPN connection as the target.
- B. Enable route propagation to the Virtual Private Gateway (VGW). ✔
- C. Enable route propagation to the customer gateway (CGW).
- D. Modify the route table of all Instances using the 'route' command.
- E. Modify the Instances VPC subnet route table by adding a route back to the customer's on-premises environment. ✔

Explanation :

Answers - B & E

Option A is incorrect because adding an option of VPN is unnecessary.

Option B is CORRECT because VGW is the other side of the connection (on the AWS side) and the route propagation needs to be enabled for the Direct Connect to work.

Option C is incorrect because the question mentions that the routes are being advertised from the customer's end. So no changes are needed at the customer side.

Option D is incorrect because there is no "route" command available on the instances in the VPC.

Option E is CORRECT because the route table needs to be updated so that the EC2 instances can communicate with the on-premise environment.

(http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/troubleshooting-response-errors.html)

Ask our Experts

QUESTION 54 UNATTEMPTED NETWORK DESIGN

You are setting up a website for a small company. This website serves up images and is very resource intensive. You have decided to serve up the images using Cloudfront. There is a requirement though, that the content should be served up using a custom domain and should work with https.

What can you do to ensure this requirement is fulfilled?

Select 2 options.

- [ ] **A.** You must provision and configure your own SSL certificate in Route 53 and associate it to your CloudFront distribution.
- [ ] **B.** You must provision Server Name Indication (SNI) Custom SSL for your CloudFront Distribution. ✔
- [ ] **C.** You must provision and configure an ALIAS in Route 53 and associate it to your CloudFront distribution ✔
- [ ] **D.** You must create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket where the images are stored.

Explanation :

Answer – B and C

Custom SSL certificate support lets you deliver content over HTTPS using your own domain name and your own SSL certificate. This gives visitors to your website the security benefits of CloudFront over an SSL connection that uses your own domain name in addition to lower latency and higher reliability.
Note: Please note that some older browsers do not support SNI and will not be able to establish a connection with CloudFront to load the HTTPS version of your content.

- https://aws.amazon.com/cloudfront/custom-ssl-domains/ (https://aws.amazon.com/cloudfront/custom-ssl-domains/)

Option C is correct. If we want to use our own domain name, we need to use Amazon Route 53 to create an alias record that points to our CloudFront distribution.

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

Option A is incorrect because custom SSL certificate or third-party certificate can not be configured in Route53.
Option D is incorrect because Origin Access identity(OAI) does not deal with custom SSL, it is only used to ensure that the origin is accessible with CloudFront distribution only.

More information on Custom SSL Domains:

AWS Cloudfront can use IAM certificates.
Reference Link:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-custom-certificate/ (https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-custom-certificate/)

Also there is a discussion forum on the same topic ""ssl certificate IAM" in the Amazon CloudFront Discussion Forum".
It is helpful in understanding about this topic further.

For more information on CloudFront custom SSL domains, please visit the below URL
https://aws.amazon.com/cloudfront/custom-ssl-domains/ (https://aws.amazon.com/cloudfront/custom-ssl-domains/)

Ask our Experts

QUESTION 55 UNATTEMPTED DEPLOYMENT MANAGEMENT

You have recently migrated an application from a customer's on-premise data center to the AWS cloud. Currently, you're using the ELB to serve traffic to the legacy application. The ELB is also using HTTP port 80 as the health check ping port. The application is currently responding by returning a website to port 80 when you test the IP address directly. However, the instance is not registering as healthy even though the appropriate amount of time has passed for the health check to register as healthy. How might the issue be resolved? Choose the correct answer from the options below

- **A.** Change the ELB listener port from ping port 80 to HTTPS port 80 for the instance to register as healthy
- **B.** Change the ELB listener port from HTTP port 80 to TCP port 80 for the instance to register as healthy ✔
- **C.** Change the ELB listener port from HTTP port 80 to HTTPS port 80 for the instance to register as healthy
- **D.** Change the ELB listener port from HTTP port 80 to TCP port 443 for the instance to register as healthy

Explanation :

Answer – B

Since the application is a custom application and not a standard HTTP application, hence you need to have the TCP ports open.
Before you start using Elastic Load Balancing, you must configure one or more *listeners* for your Classic Load Balancer. A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections, and a protocol and a port for back-end (load balancer to back-end instance) connections.
Elastic Load Balancing supports the following protocols:

- HTTP
- HTTPS (secure HTTP)
- TCP
- SSL (secure TCP)

For more information on listener configuration for ELB, please see the below link:
http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html
(http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html)

Ask our Experts

QUESTION 56 UNATTEMPTED DEPLOYMENT MANAGEMENT

Suppose you are hosting a website in an S3 bucket. Your users load the website endpoint https://website.s3-website-us-east-1.amazonaws.com. Now you want to use CSS on the web pages that are stored in a different bucket which is also public. But layout on the client browser is not loading properly. What might have gone wrong? Choose the correct option from given below

- **A.** You can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com. ✔

- **B.** Modify bucket policy on css bucket to able to access website bucket
- **C.** Modify bucket policy on website bucket to able to access css bucket
- **D.** This is not possible

Explanation :

Answer - A
Option A is CORRECT because 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 in Amazon S3, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.
Option B and C are incorrect because updating bucket policy on just one bucket does not give the CORS access to other buckets.
Option D is incorrect because this can be achieved using CORS configuration.

For more information on Cross-origin resource sharing, please refer to the below URL
http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html
(http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html)

Ask our Experts

QUESTION 57 UNATTEMPTED SECURITY

Your supervisor gave you brief of a client who needs a web application set up on AWS. The most important requirement is that MySQL must be used as the database, and this database must not be hosted in the public cloud, rather at the client's data center due to security risks. Which of the following solutions would be the best to assure that the client's requirements are met? Choose the correct answer from the options below

- **A.** Build the application server on a public subnet and the database at the client's data center. Connect them with a VPN connection which uses IPsec. ✔
- **B.** Use the public subnet for the application server and use RDS with a storage gateway to access and synchronize the data securely from the local data center.
- **C.** Build the application server on a public subnet and the database on a private subnet with a NAT instance between them.
- **D.** Build the application server on a public subnet and build the database in a private subnet with a secure ssh connection to the private subnet from the client's data center.

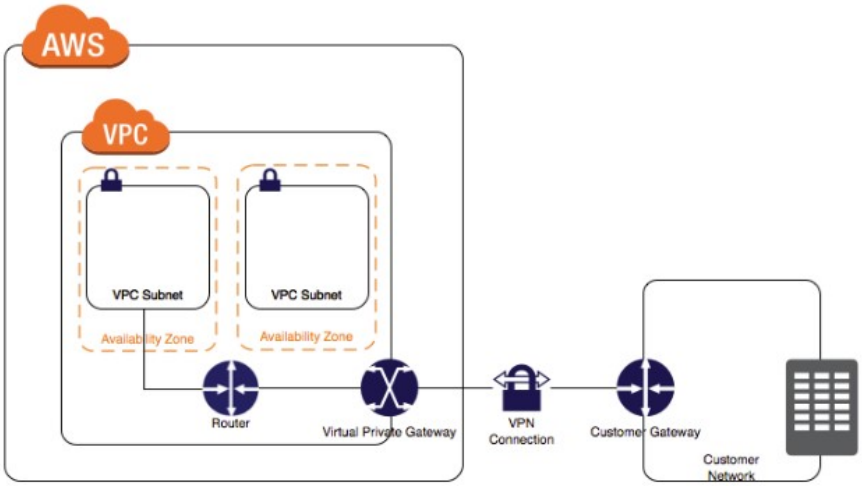
Explanation :

Answer – A

The main architectural consideration in this scenario is that the database should remain on the client's data center. Since the database should not be hosted on the cloud, you cannot put the database in any subnet in AWS.

Option A is CORRECT because it puts the application servers in public subnet and keeps the database server at the client's data center.
Option B is incorrect because MySQL must be used as the database. Also, configuring the storage gateway is an unnecessary overhead.
Option C is incorrect because the requirement is to keep the database server at the client's data center. So you cannot put it in any AWS VPC subnet.
Option D is incorrect because building the database in private subnet and accessing the database server at client's data center via ssh is totally unnecessary and non-feasible.

The best option is to create a VPN connection for securing traffic as shown below



For more information on VPN connections, please visit the below URL
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
(http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts

QUESTION 58 UNATTEMPTED SECURITY

Regarding encryption on data stored on your databases, namely Amazon RDS, which of the following statements is the true? Choose the correct answer from the options below

- **A.** Encryption cannot be enabled on RDS instances unless the keys are not managed by KMS.

- **B.** Encryption can be enabled on RDS instances to encrypt the underlying storage, and this will by default also encrypt snapshots as they are created. No additional configuration needs to be made on the client side for this to work. ✔
- **C.** Encryption can be enabled on RDS instances to encrypt the underlying storage, and this will by default also encrypt snapshots as they are created. However, some additional configuration needs to be made on the client side for this to work.
- **D.** Encryption can be enabled on RDS instances to encrypt the underlying storage, but you cannot encrypt snapshots as they are created.

Explanation :

Answer – B

Tip for the exam: You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance (only certain EC2 instance types support encryption, more information is given below). Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, Read Replicas, and snapshots.

Option A is incorrect because the RDS instance encryption supports only those Master Keys that are created and managed by KMS.
Option B is CORRECT because once the encryption is enabled, its automated backups, read replicas, and snapshots are automatically encrypted without need of any addition settings.
Option C is incorrect because no additional configurations need to be made from client side, once the encryption is enabled.
Option D is incorrect because, as mentioned above, the snapshots get automatically encrypted once the encryption is turned-on on the RDS instance.

For more information on RDS encryption, please visit the below url
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
(http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html)
See the list of instance types that support the encryption:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availal
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html#Overview.Encryption.Availa

Ask our Experts

QUESTION 59 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

You are setting up a VPN for a customer to connect his remote network to his Amazon VPC environment. There are many ways to accomplish this. Also, you have given a list of the things that the customer has specified that the network needs to be able to do. They are as follows:

- Predictable network performance

- Support for BGP peering and routing policies

- A secure IPsec VPN connection but not over the Internet

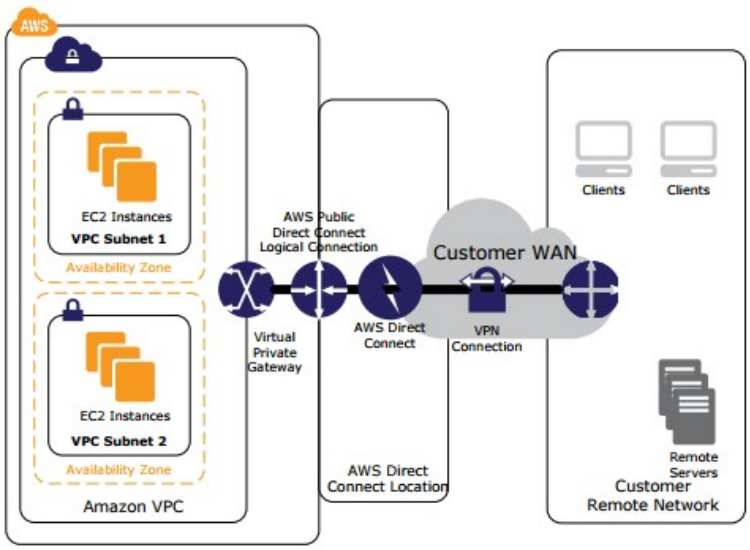
Which of the following VPN options would best satisfy the customer's requirements? Choose the correct answer from the options below

- **A.** Software appliance-based VPN connection with IPsec
- **B.** AWS Direct Connect and IPsec Hardware VPN connection not over the internet. ✔
- **C.** AWS Direct Connect with AWS VPN CloudHub
- **D.** AWS VPN CloudHub

Explanation :

Answer – B

Since one of the requirements does not use the internet, Option A and D is not advisable since they would traverse over the internet, and the internet connectivity always has unpredictability as one of the factors.
Since there is a need for predictable network performance, AWS Direct connect becomes the best option. Along with a Hardware VPN connection, it can create the secure VPN connection that is demanded. See the image below:



Option A and D are incorrect because both approaches uses internet connectivity - which is not what the scenario wants to use.
Option B is CORRECT because (a) with AWS Direct Connect, you would always get the predictable network performance without using the internet, and (b) it uses Hardware VPN Connection which is a secure way of logging into the AWS platform.

Option C is incorrect because CloudHub is used when your remote sites want to communicate with each other, and not just with the AWS VPC. AWS Direct Connect with Hardware VPN is the best architectural solution here.

There is a good read on different connection options for AWS. Please visit the below URL on the same.
https://d0.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-options.pdf (https://d0.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-options.pdf)
More information on AWS CloudHub:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html)

Ask our Experts

QUESTION 60 UNATTEMPTED SECURITY

Your security officer has told you that you need to tighten up the logging of all events that occur on your AWS account. He wants to be able to access all events that occur on the account across all regions quickly and in the simplest possible manner. He also wants to make sure he is the only person that has access to these events in the most secure way possible. Which of the following would be the best solution to assure his requirements are met? Choose the correct answer from the options below

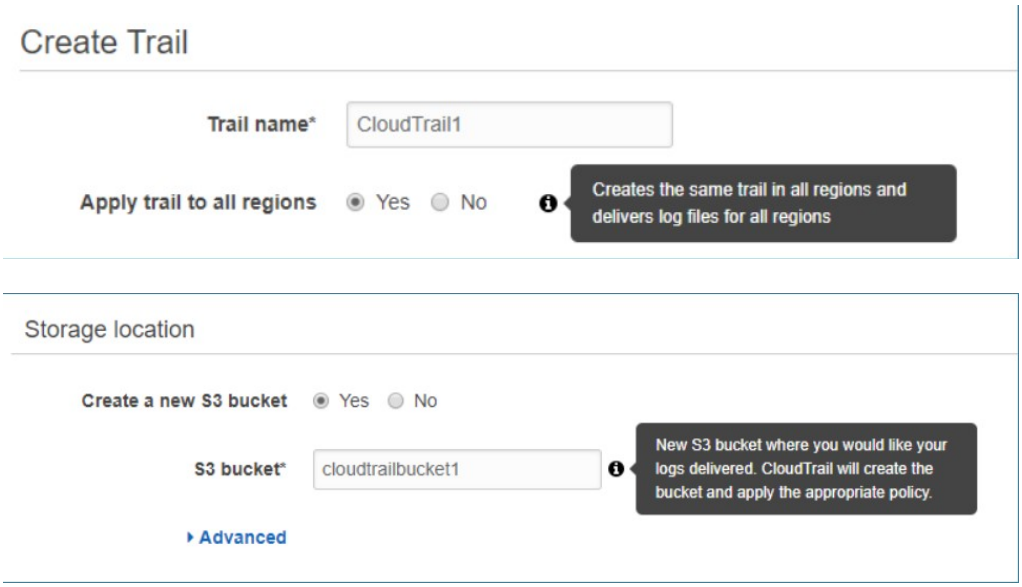
- **A.** Use CloudTrail to log all events to one S3 bucket. Make this S3 bucket only accessible by your security officer with a bucket policy that restricts access to his user only and also add MFA to the policy for a further level of security. ✔
- **B.** Use CloudTrail to log all events to an Amazon Glacier Vault. Make sure the vault access policy only grants access to the security officer's IP address.
- **C.** Use CloudTrail to send all API calls to CloudWatch and send an email to the security officer every time an API call is made. Make sure the emails are encrypted.
- **D.** Use CloudTrail to log all events to a separate S3 bucket in each region as CloudTrail cannot write to a bucket in a different region. Use MFA and bucket policies on all the different buckets.

Explanation :

Answer – A

The main points to consider in this scenario is: (1) the security officer needs to access all events that occur on the account **across all the regions**, and (2) only that security officer should have the access.

Option A is CORRECT because it configures only one S3 bucket for all the CloudTrail log events on the account across all the regions. It also restricts the access to the security officer only via the bucket policy. See the images below:



Option B is incorrect because it uses Amazon Glacier vaults which is an archival solution and not used for storing the CloudTrail logs .
Option C is incorrect because sending the API calls to CloudWatch is unnecessary. Also notifying the security officer via email is not a good nor a secure architecture.
Option D is incorrect because CloudTrail provides with an option where are all the logs get delivered to a single S3 bucket. Putting all the logs in separate buckets is an overhead .

More information on AWS CloudTrail
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.
You can design CloudTrail to send all logs to a central S3 bucket.
For more information on CloudTrail, please visit the below URL
https://aws.amazon.com/cloudtrail/ (https://aws.amazon.com/cloudtrail/)

Ask our Experts

QUESTION 61 UNATTEMPTED DEPLOYMENT MANAGEMENT

You have created a temporary application that accepts image uploads, stores them in S3, and records information about the image in RDS. After building this architecture and accepting images for the duration required, it's time to delete the CloudFormation template. However, your manager has informed you that for archival reasons the RDS data needs to be stored and the S3 bucket with the images needs to remain. Your manager has also instructed you to ensure that the application can be restored by a CloudFormation template and run next year during the same period.

Knowing that when a CloudFormation template is deleted, it will remove the resources it created, what is the best method to achieve the desired goals? Choose the correct answer from the options below

- **A.** Enable S3 bucket replication on the source bucket to a destination bucket to maintain a copy of all the S3 objects, set the deletion policy for the RDS instance to snapshot.
- **B.** For both the RDS and S3 resource types on the CloudFormation template, set the DeletionPolicy to Retain
- **C.** Set the DeletionPolicy on the S3 resource to snapshot and the DeletionPolicy on the RDS resource to snapshot.
- **D.** Set the DeletionPolicy on the S3 resource declaration in the CloudFormation template to retain, set the RDS resource declaration DeletionPolicy to snapshot. ✔

Explanation :

Answer - D

The main points in this scenario are: even if the CloudFormation stack is deleted, (1) the RDS data needs to be stored, and (2) the S3 bucket with the images should remain (not be deleted).
Option A is incorrect because even if the images are backed up to another bucket, the original bucket would be deleted if the CloudFormation stack is deleted. One of the requirements is to retain the S3 bucket.
Option B is incorrect because DeletionPolicy attribute for RDS should be *snapshot*, not *retain* because with *snapshot* option, the backup of the RDS instance would be stored in the form of snapshots (which is the requirement). With *retain* option, CF will keep the RDS instance alive which is unwanted.
Option C is incorrect because the DeletionPolicy of the S3 bucket should be *retain*, not *snapshot*.
Option D is CORRECT because it correctly sets the DeletionPolicy of *retain* on S3 bucket and *snapshot* on RDS instance.
More information on DeletionPolicy on CloudFormation

DeletionPolicy options include:

- **Retain**: You retain the resource in the event of a stack deletion.
- **Snapshot**: You get a snapshot of the resource before it's deleted. This option is available only for resources that support snapshots.
- **Delete**: You delete the resource along with the stack. This is the default outcome if you don't set a DeletionPolicy.

AWS Document says:
To keep or copy resources when you delete a stack, you can specify either the Retain or Snapshot policy options.

With the DeletionPolicy attribute, you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default.

To keep a resource when its stack is deleted, specify Retain for that resource. You can use retain for any resource. For example, you can retain a nested stack, Amazon S3 bucket, or EC2 instance so that you can continue to use or modify those resources after you delete their stacks.
Note
If you want to modify resources outside of AWS CloudFormation, use a retain policy and then delete the stack. Otherwise, your resources might get out of sync with your AWS CloudFormation template and cause stack errors.
For resources that support snapshots, such as AWS::EC2::Volume, specify Snapshot to have AWS CloudFormation create a snapshot before deleting the resource.
For more information on Cloudformation deletion policy, please visit the below URL
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html (http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html)

Ask our Experts

QUESTION 62 UNATTEMPTED SECURITY

An auditor has been advised to go through the VPC artifacts in your AWS account. Which of the below options should be carried out so that the auditor can carry out the audit? Choose the correct answer from the options below.

- **A.** Create an IAM user tied to an administrator role. Also provide an additional level of security with MFA.
- **B.** Give the auditor root access to your AWS Infrastructure, because an auditor will always need access to every service.
- **C.** Create an IAM Role with the read only permissions to access the AWS VPC infrastructure and assign that role to the auditor. ✔
- **D.** Create an IAM user with full VPC access but set a condition that will not allow the auditor to modify anything if the request is from any IP other than their own.

Explanation :

Answer – C

Generally, you should refrain from giving high-level permissions and give only the required permissions. In this case, option C fits well by just providing the relevant access which is required.

Option A is incorrect because you should create an IAM Role with the needed permissions.
Option B is incorrect because you should not give the root access as it will give the user full access to all AWS resources.
Option C is CORRECT because IAM Role gives just the minimum required permissions (read-only) to audit the VPC infrastructure to the auditor.
Option D is incorrect because you should not give the auditor full access to the VPC.

For more information on Identity and Access Management, please visit the below URL

https://aws.amazon.com/iam/ (https://aws.amazon.com/iam/)

Ask our Experts

QUESTION 63 UNATTEMPTED DATA STORAGE

You are launching your first ElastiCache cache cluster, and start using Memcached. Which of the following is NOT a key features of Memcache. Choose the correct answer from the options below

- **A.** You need the ability to scale your cache horizontally as you grow.
- **B.** You use more advanced data types, such as lists, hashes, and sets. ✔
- **C.** You need as simple a caching model as possible.
- **D.** Object caching is your primary goal to offload your database.

Explanation :

Answer – B
Option B is CORRECT because it is Redis, not Memcached,which supports advanced/complexdata types such as strings, hashes, lists, sets, sorted sets, and bitmaps.
Option A, C and D are all incorrect because these are the main features of Memcached.

For the exam, it is very important to remember the differences between Memcached and Redis. Both are excellent solutions, but used for different scenarios. Please see the notes given below by the AWS documentation:

Choose Memcached if the following apply to your situation:

- You need the simplest model possible.
- You need to run large nodes with multiple cores or threads.
- You need the ability to scale out/in, adding and removing nodes as demand on your system increases and decreases.
- You need to cache objects, such as a database.

Choose Redis 2.8.x or Redis 3.2.4 (non-clustered mode) if the following apply to your situation:

- You need complex data types, such as strings, hashes, lists, sets, sorted sets, and bitmaps.
- You need to sort or rank in-memory data-sets.
- You need persistence of your key store.
- You need to replicate your data from the primary to one or more read replicas for read intensive applications.
- You need automatic failover if your primary node fails.
- You need publish and subscribe (pub/sub) capabilities—to inform clients about events on the server.
- You need backup and restore capabilities.
- You need to support multiple databases.

For more information on the various caching engines, please visit the below url
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/SelectEngine.Uses.html
(http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/SelectEngine.Uses.html)

Ask our Experts

QUESTION 64 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

A new client may use your company to move all their existing Data Center applications and infrastructure to AWS. This is going to be a huge contract for your company, and you have been handed the entire contract and need to provide an initial scope to this possible new client. One of the things you notice concerning the existing infrastructure is that it has few legacy applications that you are almost certain will not work on AWS. Which of the following would be the best strategy to employ regarding the migration of these legacy applications? Choose the correct answer from the options below

- **A.** Create two VPCs. One containing all the legacy applications and the other containing all the other applications. Make a connection between them with VPC peering.
- **B.** Move the legacy applications onto AWS first, before you build any infrastructure. There is sure to be an AWS Machine Image that can run this legacy application.
- **C.** Create a hybrid cloud by configuring a VPN tunnel to the on-premises location of the Data Center. ✔
- **D.** Convince the client to look for another solution by de-commissioning these applications and seeking out new ones that will run on AWS.

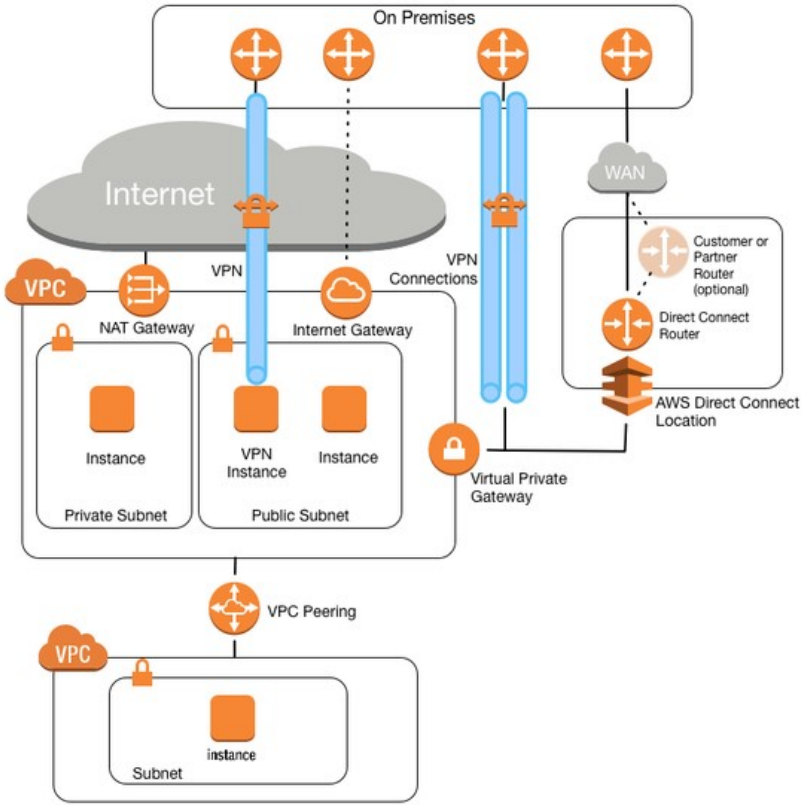
Explanation :

Answer – C

Option A is incorrect because, there are some legacy application that will not work on AWS platform. So creating VPC for such applications will not be possible.
Option B is incorrect because the scenario explicitly mentions that there are some components of the application (legacy part) that will not work with AWS. So, it is highly presumptuous that the legacy application can be run by an AWS Machine Image (legacy application may consist of more than just AMIs).
Option C is CORRECT because it uses hybrid approach - where the legacy application stays on-premises. It should definitely work as the remaining infrastructure would be on AWS. The communication between the two infrastructures would be taken care by establishing the VPN connection. This is certainly the most viable, time and cost saving solution among the given options.
Option D is incorrect because it is the least feasible solution. First of all, de-comissioning the legacy application may not be possible for the client; especially when the scenario says that the legacy application is almost surely not going to work on AWS. Still, even if they agree, it would be a big impact

on the client in terms of time, cost and efforts to re-architect the solution to replace the legacy application.

More information on the hybrid setup:
The best option is to have a dual mode wherein you have the legacy apps running on-premise and start migrating the apps which have compatibility in the cloud. Have a VPN connection from the on-premise to the cloud for ensuring communication can happen from each environment to the other.



For the full fundamentals on AWS networking options, please visit the URL:
https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/
(https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/)

Ask our Experts

QUESTION 65 UNATTEMPTED SECURITY

You're building a mobile application game. The application needs permission for each user to communicate and store data in DynamoDB tables. What is the best method for granting each mobile device (that installs your application) to access DynamoDB tables for storage when required?

Choose the correct answer from the options below

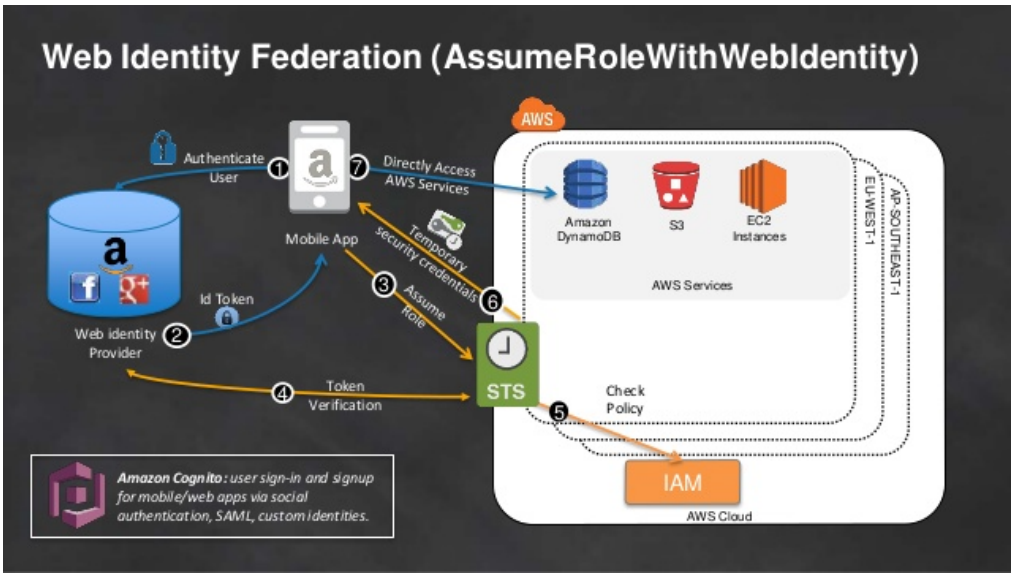
- **A.** During the install and game configuration process, have each user create an IAM credential and assign the IAM user to a group with proper permissions to communicate with DynamoDB.
- **B.** Create an IAM group that gives access to your application and to the DynamoDB tables. Then, when writing to DynamoDB, simply include the unique device ID to associate the data with that specific user.
- **C.** Create an IAM role with the proper permission policy to communicate with the DynamoDB table. Use web identity federation, which assumes the IAM role using AssumeRoleWithWebIdentity, when the user signs in, granting temporary security credentials using STS. ✔
- **D.** Create an Active Directory server and an AD user for each mobile application user. When the user signs in to the AD sign-on, allow the AD server to federate using SAML 2.0 to IAM and assign a role to the AD user which is the assumed with AssumeRoleWithSAML.

Explanation :

Answer – C

Option A is incorrect because IAM Roles are preferred over IAM Users, because IAM Users have to access the AWS resources using access and secret keys, which is a security concern.
Option B is this is not a feasible configuration.
Option C is CORRECT because it (a) creates an IAM Role with the needed permissions to connect to DynamoDB, (b) it authenticates the users with Web Identity Federation, and (c) the application accesses the DynamoDB with temporary credentials that are given by STS.
Option D is incorrect because the step to create the Active Directory (AD) server and using AD for authenticating is unnecessary and costly.

See the image below for more information on AssumeRoleWithWebIdentity API



For more information on AssumeRolewithWebIdentity, please visit the below URL

http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html (http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html)

Ask our Experts

QUESTION 66 UNATTEMPTED DATA STORAGE

You have been given the task of designing a backup strategy for your organization's on-premise storage with the only caveat being that you must use the AWS storage Gateway. Which of the following is the correct/appropriate statement surrounding the backup strategy on the AWS Storage Gateway? Choose the correct answer from the options below

- **A.** You should use the Gateway-Virtual Tape Library (VTL) since the Gateway-Cached Volumes and Gateway-Stored Volumes cannot be used for backups.
- **B.** You should use Gateway-Cached Volumes. You will have quicker access to the data, and it is a more preferred backup solution than Gateway-Stored Volumes.
- **C.** It doesn't matter whether you use Gateway-Cached Volumes or Gateway-Stored Volumes as long as you also combine either of these solutions with the Gateway-Virtual Tape Library (VTL).
- **D.** You should use Gateway-Stored Volumes as it is preferable to Gateway-Cached Volumes as a backup storage medium. ✔

Explanation :

Answer - D

Option A is incorrect because Gateway-Stored Volumes are used for backing up the data from on-premises to the Amazon S3.
Option B is incorrect because it keeps only the frequently accessed data (not the entire data) on the on-premises server to which you get the quick access.
Option C is incorrect because both Gateway-Cached Volume as well as Gateway-Stored Volume can be independently deployed as storage/backup options and need not necessarily be combined with VTL.
Option D is CORRECT because (a) the scenario in the question is asking you to design a backup (not a storage) strategy, (b) Gateway-Stored Volume *backs up* the data on Amazon S3 while keeping the data on the on-premises server, and (c) Gateway-Cached Volume only keeps the frequently accessed data on the on-premises server and *stores* the data on Amazon S3.

More information on AWS Storage Gateway

Volume Gateway – A volume gateway provides cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. The gateway supports the following volume configurations:

- Cached volumes – You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data.
- Stored volumes – If you need low-latency access to your entire dataset, first configure your on-premises gateway to store all your data locally. Then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive offsite backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

Tape Gateway – With a tape gateway, you can cost-effectively and durably archive backup data in Amazon Glacier. A tape gateway provides a virtual tape infrastructure that scales seamlessly with your business needs and eliminates the operational burden of provisioning, scaling, and maintaining a physical tape infrastructure.

For more information on Storage gateways, please visit the below URL:
https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html (https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html)
https://aws.amazon.com/storagegateway/faqs/ (https://aws.amazon.com/storagegateway/faqs/)

Ask our Experts

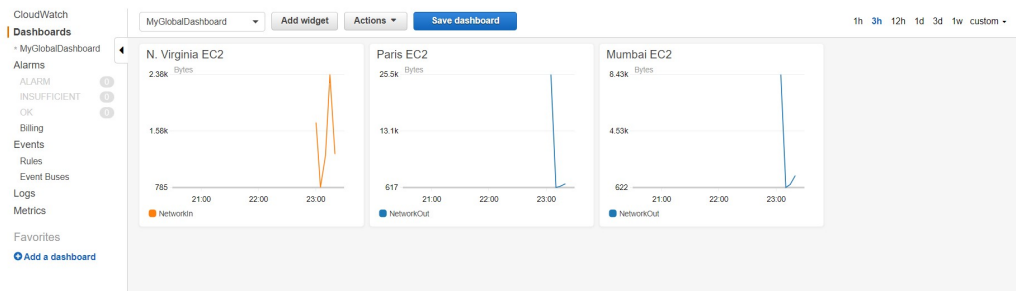
QUESTION 67 UNATTEMPTED DEPLOYMENT MANAGEMENT

Your company has an e-commerce platform which is expanding all over the globe, you have EC2 instances deployed in multiple regions you want to monitor the performance of all of these EC2 instances. How will you setup CloudWatch to monitor EC2 instances in multiple regions?

- A. Create separate dashboards in every region
- B. Register instances running on different regions to CloudWatch
- C. Have one single dashboard that reports the metrics from CloudWatch pertaining to different regions ✔
- D. This is not possible

Explanation :

Answer – C
You can monitor AWS resources in multiple regions using a single CloudWatch dashboard. For example, you can create a dashboard that shows CPU utilization for an EC2 instance located in the us-west-2 region with your billing metrics, which are located in the us-east-1 region.
Please see the following snapshot which shows how a global CloudWatch Dashboard looks:



For more information on Cloudwatch dashboard, please refer to the below URL
http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cross_region_dashboard.html
(http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cross_region_dashboard.html)

Ask our Experts

QUESTION 68 UNATTEMPTED DEPLOYMENT MANAGEMENT

What does the below custom IAM Policy achieve?

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
```

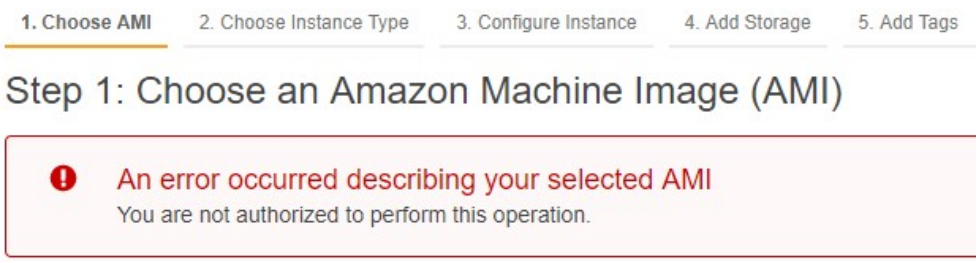
```
    "Resource": "*"
  }
 ]
}
```

- **A.** Permits the user start, stop, terminate and describe the existing instances. ✔
- **B.** Permits the user to launch a new instance as well as start, stop, and terminate the existing instances.
- **C.** Permits the user to only describe the instances (read only), and will not be able to start, stop, or terminate instances, since it overrides the allowed actions of TerminateInstances, RunInstances, StartInstances, and StopInstances in the policy.
- **D.** None of the above.

Explanation :

Answer – A

- Option A is CORRECT because, although the policy given in the question allows the access to launch the EC2 instance by including "ec2:RunInstances" in the Actions, it will not allow the user to launch the EC2 instances. (Try creating the same policy, attach it to a new user. You can login using that user credentials and see if you can launch any EC2 instance. You will not be able to do so. You will get the error shown below.). In order to allow users to launch an instance, the policy needs to be updated to grant the user more privileges: access to launch using an EC2 key pair, a security group, an Elastic Block Store (EBS) volume, and an Amazon Machine Image (AMI). To do this, you will have to create a separate statement for the RunInstances action.
- Option B is incorrect because, as mentioned above, the user will not be able to launch any EC2 instance and will get an error (shown below) about not having the permission to do so.



- Option C is incorrect because the user can start, stop, and terminate existing instances with this policy.
- Option D is incorrect because the user will be able to start, stop and terminate existing EC2 instances.

For more information on EC2 resource-level permissions please visit the below URL and for further explanation as to why only the TerminateInstances, StopInstances, and StartInstances actions are allowed please visit the below URL

- https://aws.amazon.com/blogs/security/demystifying-ec2-resource-level-permissions/ (https://aws.amazon.com/blogs/security/demystifying-ec2-resource-level-permissions/)

Ask our Experts

QUESTION 69 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

A company is running a production load Redshift cluster for a client. The client has an RTO objective of one hour and an RPO of one day. While configuring the initial cluster what configuration would best meet the recovery needs of the client for this specific Redshift cluster configuration? Choose the correct answer from the options below

- **A.** Enable automatic snapshots on the cluster in the production region FROM the disaster recovery region so snapshots are available in the disaster recovery region and can be launched in the event of a disaster.
- **B.** Enable automatic snapshots and configure automatic snapshot copy from the current production cluster to the disaster recovery region. ✔
- **C.** Enable automatic snapshots on a Redshift cluster. In the event of a disaster, a failover to the backup region is needed. Manually copy the snapshot from the primary region to the secondary region.
- **D.** Create the cluster configuration and enable Redshift replication from the cluster running in the primary region to the cluster running in the secondary region. In the event of a disaster, change the DNS endpoint to the secondary cluster's leader node.

Explanation :

Answer – B

Option A is incorrect because it copies the snapshot from the destination region (disaster recovery region).
Option B is CORRECT because it copies the snapshot from source region (production) to the destination region (disaster recovery region).
Option C is incorrect because you do not need to copy the manual snapshots (as it is an overhead), Redshift copies the snapshot from source to destination region.
Option D is incorrect because Redshift replicates the data to another region using snapshots. Once the snapshot is copied from the source to destination region, you need to restore cluster from the snapshot and use its DSN.

More information on Amazon Redshift Snapshots
Snapshots are point-in-time backups of a cluster. There are two types of snapshots: *automated* and *manual*. Amazon Redshift stores these snapshots internally in Amazon S3 by using an encrypted Secure Sockets Layer (SSL) connection. If you need to restore from a snapshot, Amazon Redshift creates a new cluster and imports data from the snapshot that you specify.
When you restore from a snapshot, Amazon Redshift creates a new cluster and makes the new cluster available before all of the data is loaded, so you can begin querying the new cluster immediately. The cluster streams data on demand from the snapshot in response to the active queries then loads the remaining data in the background.
Amazon Redshift periodically takes snapshots and tracks incremental changes to the cluster since the last snapshot. Amazon Redshift retains all of the data required to restore a cluster from a snapshot.
For more information on RedShift snapshots, please visit the below URL
http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html

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

Ask our Experts

QUESTION 70 UNATTEMPTED COSTING

A company runs their current application entirely on-premise. However, they are expecting a big boost in traffic and need to figure out a way to decrease the load to handle the scale. Unfortunately, they cannot migrate their application to AWS in the period required. What could they do with their current on-premise application to help offload some of the traffic and scale to meet the demand expected in 24 hours in a cost-effective way? Choose the correct answer from the options below.

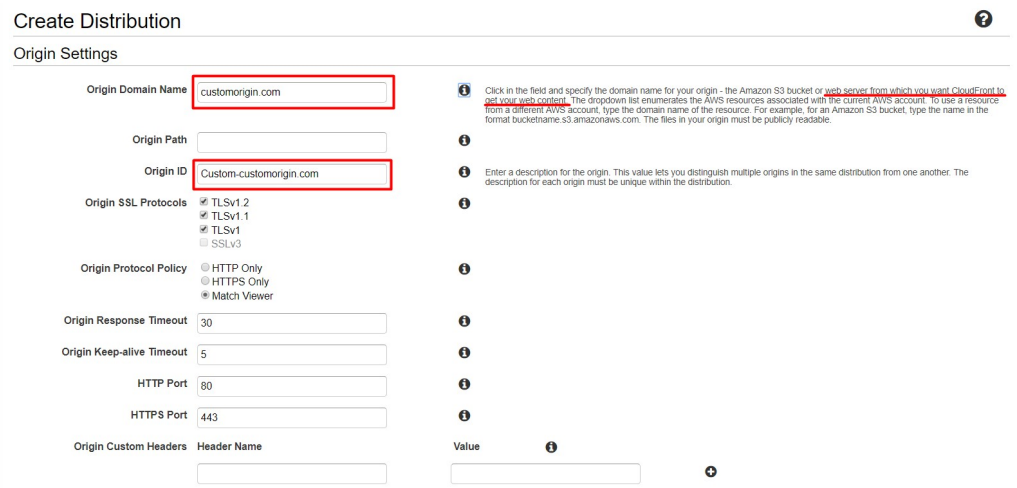
- **A.** Deploy OpsWorks on-premise to manage the instance in order to configure on-premise auto scaling to meet the demand.
- **B.** Upload all static files to Amazon S3 and create a CloudFront distribution serving those static files.
- **C.** Duplicate half your web infrastructure on AWS, offload the DNS to Route 53 and configure weighted based DNS routing to send half the traffic to AWS .
- **D.** Create a CloudFront CDN, enable query string forwarding and TTL of zero on the origin. Offload the DNS to AWS to handle CloudFront CDN traffic but use on-premise load balancers as the origin. ✔

Explanation :

Answer – D

The main point to consider is that the application should entirely stay on the on-premises server but still leverage AWS offerings for handling the peak traffic and scale on demand. CloudFront is best suited for such situation because it can use the on-premises server as the custom origin.

Option A is incorrect because even though OpsWork can work with on-premises servers, setting up the EC2 instances with Auto Scaling would be a costly solution.
Option B is incorrect because moving to static files to S3 is not sufficient to improve the scalability to handle the peak load.
Option C is incorrect because the requirement explicitly mentions that the application cannot be migrated to AWS.
Option D is CORRECT because CloudFront - which is an AWS managed - is a highly available, scalable service that can use the on-premises server as the origin. By setting the TTL to 0, the content will be delivered from the origin as soon as it gets changed. See the image below:



For more information on CloudFront, please visit the below URL
https://aws.amazon.com/cloudfront/ (https://aws.amazon.com/cloudfront/)
https://aws.amazon.com/blogs/aws/amazon-cloudfront-support-for-custom-origins/
(https://aws.amazon.com/blogs/aws/amazon-cloudfront-support-for-custom-origins/)

Ask our Experts

QUESTION 71 UNATTEMPTED CLOUD MIGRATION & HYBRID ARCHITECTURE

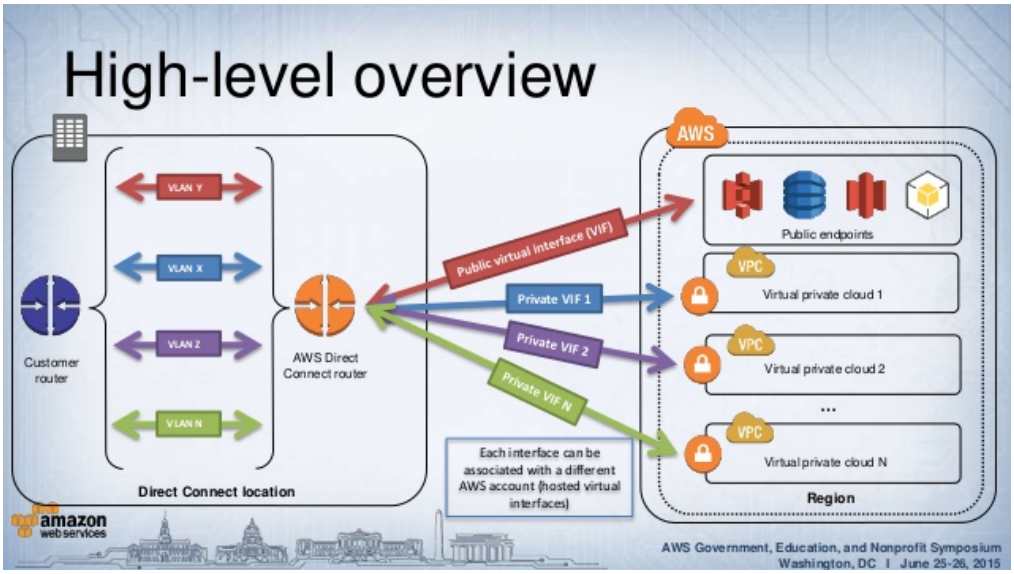
If one needs to establish a low latency dedicated connection to an S3 public endpoint over the Direct Connect dedicated low latency connection, what steps need to be taken to accomplish configuring a direct connection to a public S3 endpoint? Choose the correct answer from the options below (https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.

- **A.** Configure a public virtual interface to connect to a public S3 endpoint resource. ✔
- **B.** Establish a VPN connection from the VPC to the public S3 endpoint.
- **C.** Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.
- **D.** Add a BGP route as part of the on-premise router; this will route S3 related traffic to the public S3 endpoint to dedicated AWS region.

Explanation :

Answer – A

You can create a public virtual interface to connect to public resources or a private virtual interface to connect to your VPC. You can configure multiple virtual interfaces on a single AWS Direct Connect connection, and you'll need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key. See the image below:



Option A is CORRECT because, as mentioned above, it creates a public virtual interface to connect to S3 endpoint.
Option B is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not VPN.
Option C is incorrect because to connect to S3 endpoint, a **public** virtual interface needs to be created, **not private**.
Option D is incorrect because this setup will not help connecting to the S3 endpoint.

For more information on virtual interfaces, please visit the below URL
http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html
(http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html)

Ask our Experts

QUESTION 72 UNATTEMPTED COSTING

A company has a Redshift cluster for petabyte-scale data warehousing. The data within the cluster is easily reproducible from additional data stored on Amazon S3. The company wants to reduce the overall total cost of running this Redshift cluster. Which scenario would best meet the needs of the running cluster, while still reducing total overall ownership cost of the cluster? Choose the correct answer from the options below

- **A.** Instead of implementing automatic daily backups, write a CLI script that creates manual snapshots every few days. Copy the manual snapshot to a secondary AWS region for disaster recovery situations.
- **B.** Enable automated snapshots but set the retention period to a lower number to reduce storage costs
- **C.** Implement daily backups, but do not enable multi-region copy to save data transfer costs.
- **D.** Disable automated and manual snapshots on the cluster ✔

Explanation :

Answer – D
Snapshots are point-in-time backups of a cluster. There are two types of snapshots: *automated* and *manual*. Amazon Redshift stores these snapshots internally in Amazon S3 by using an encrypted Secure Sockets Layer (SSL) connection. If you need to restore from a snapshot, Amazon Redshift creates a new cluster and imports data from the snapshot that you specify.
Now since the question already mentions that the cluster is easily reproducible from additional data stored on Amazon S3 then you don't need to maintain any sort of snapshots.

Option A is incorrect because (a) manual snapshots are going to be costly, ans (b) since the cluster can be reproducible from the data stored in S3, the step copying to another region is not needed.
Option B is incorrect because taking automated snapshots is an expensive solution here.
Option C is incorrect because implementing daily backup is going to be expensive as well.
Option D is CORRECT because taking any of automated and manual snapshots is unnecessary as the cluster can easily be restored via the data stored in S3. Hence, once the snapshot taking is disabled, the cost would be lowered.

For more information on Redshift snapshots, please visit the below URL
http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html
(http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html)

Ask our Experts

QUESTION 73 UNATTEMPTED SCALABILITY & ELASTICITY

A company is running a web application that has a high amount of dynamic content. The company is looking to reduce load time by implementing a caching solution that will help reduce load times for clients requesting the application. What is the best possible solution and why? Choose the correct answer from the options below

- **A.** Offload the DNS to Route 53; Route 53 has DNS servers all around the world and routes the request to the closest region which reduces DNS latency.

- **B.** Create an ElastiCache cluster, write code that caches the correct dynamic content and places it in front of the RDS dynamic content. This will reduce the amount of time it takes to request the dynamic content since it is cached.
- **C.** Create a CloudFront distribution, enable query string forwarding, set the TTL to 0: This will keep TCP connections open from CloudFront to origin, reducing the time it takes for TCP handshake to occur. ✔
- **D.** Create a CloudFront distribution; disable query string forwarding, set the TTL to 0. This will keep TCP connections open from CloudFront to origin, reducing the time it takes for TCP handshake to occur

Explanation :

Answer – C
The scenario requires a caching solution which should help reducing the load time of the dynamic content. Although ElastiCache is a good solution for caching, it is most suited for caching the static content so that the read intensive load is reduced on the database instance. CloudFront is a good solution to improve the performance of a distributed application that has a high amount of dynamic content.

- Option A is incorrect because Route 53 helps improving the resolving of the DNS queries for the multi-region application. It does not help caching of the dynamic content.
- Option B is incorrect because ElastiCache is most suited for caching the static content so that the read intensive load is reduced on the database instance.
- Option C is CORRECT because (a) it uses CloudFront distribution which is AWS managed highly available and scalable service, (b) it sets the TTL to 0, so that whenever the content changes at the origin, the updated content immediately gets cached at all the edge locations, giving users the latest content, and (c) it uses query string forwarding to get the custom or dynamic content generated at the origin server using the query string parameters.

Note:
AWS states that,
If you set the TTL for a particular origin to 0, CloudFront will still cache the content from that origin. It will then make a GET request with an If-Modified-Since header, thereby giving the origin a chance to signal that CloudFront can continue to use the cached content if it hasn't changed at the origin.

Variable Time-To-Live (TTL) – In many cases, dynamic content is either not cacheable or cacheable for a very short period of time, perhaps just a few seconds. In the past, CloudFront's minimum TTL was 60 minutes since all content was considered static. The new minimum TTL value is 0 seconds. If you set the TTL for a particular origin to 0, CloudFront will still cache the content from that origin. It will then make a GET request with an If-Modified-Since header, thereby giving the origin a chance to signal that CloudFront can continue to use the cached content if it hasn't changed at the origin.
Please refer the following link for more information.

- https://aws.amazon.com/blogs/aws/amazon-cloudfront-support-for-dynamic-content/ (https://aws.amazon.com/blogs/aws/amazon-cloudfront-support-for-dynamic-content/)

Ask our Experts

QUESTION 74 UNATTEMPTED DATA STORAGE

You are running an online gaming server, with one of its requirements being a need for 100,000 IOPS of write performance on its EBS volumes. Given the fact that EBS volumes can only provision a maximum of up to 20,000 IOPS which of the following would be a reasonable solution if instance bandwidth is not an issue? Choose the correct answer from the options below

- A. Create a RAID 0 configuration for five 20,000 IOPS EBS volumes. ✔
- B. Use ephemeral storage which gives a much larger IOPS write performance.
- C. Use Auto Scaling to use spot instances when required to increase the IOPS write performance when required.
- D. Create a Placement Group with five 20,000 IOPS EBS volumes.

Explanation :

Answer – A

Option A is CORRECT because creating a RAID 0 array allows you to achieve a higher level of performance for a file system than you can provision on a single Amazon EBS volume and the resulting size of a RAID 0 array is the sum of the sizes of the volumes within it, and the bandwidth is the sum of the available bandwidth of the volumes within it.
Option B is incorrect because ephemeral storage may not always have consistent and reliable I/O performance as given by PIOPS EBS Volumes.
Option C is incorrect because (a) instance bandwidth is not an issue, and (b) auto-scaling with spot instances will not increase the IOPS of the EBS volumes.
Option D is incorrect because launching the instances in a placement group does not increase the IOPS of the EBS volumes, it only increases the overall network performance.

More information on EBS with RAID Configuration
With Amazon EBS you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together.
An example of better throughout with RAID 0 configuration is also given in the AWS documentation
The resulting size of a RAID 0 array is the sum of the sizes of the volumes within it, and the bandwidth is the sum of the available bandwidth of the volumes within it. The resulting size and bandwidth of a RAID 1 array is equal to the size and bandwidth of the volumes in the array. For example, two 500 GiB Amazon EBS io1 volumes with 4,000 provisioned IOPS each will create a 1000 GiB RAID 0 array with an available bandwidth of 8,000 IOPS and 1,000 MB/s of throughput or a 500 GiB RAID 1 array with an available bandwidth of 4,000 IOPS and 500 MB/s of throughput.
For more information on RAID configuration, please visit the below URL:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html)

Ask our Experts

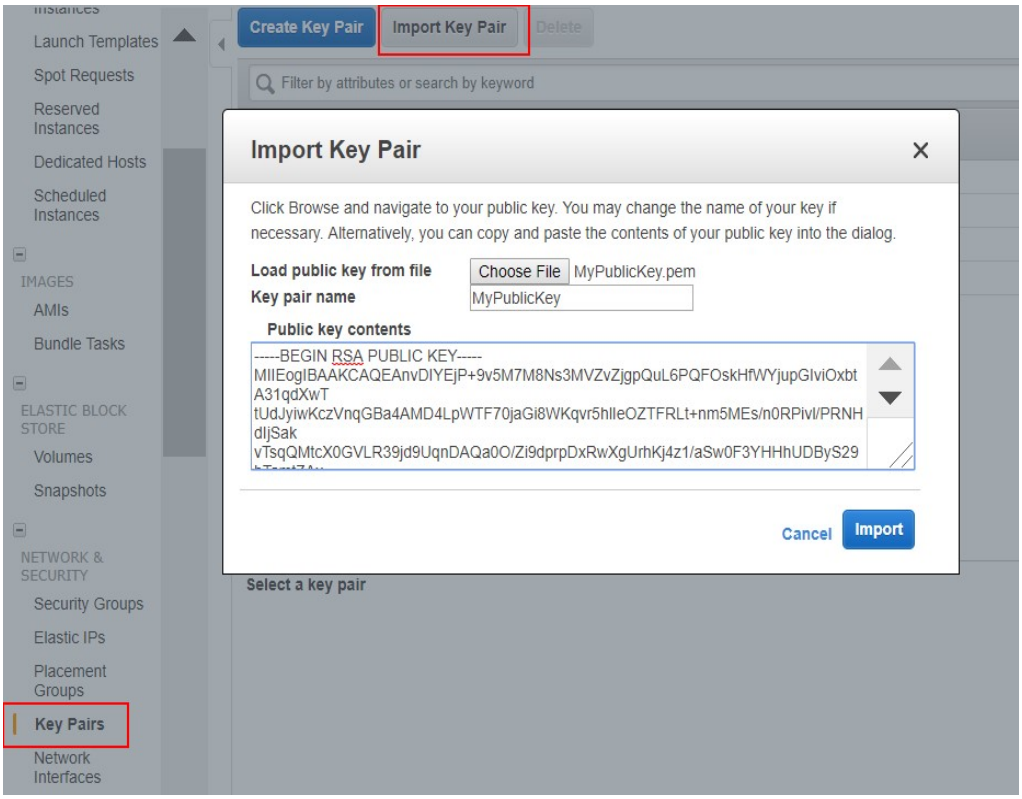
QUESTION 75 UNATTEMPTED DEPLOYMENT MANAGEMENT

While implementation of cost-cutting measurements in your organization, you have been told that you need to migrate some of your existing resources to another region. The first task you have been given is to copy all of your Amazon Machine Images from Asia Pacific (Sydney) to US West (Oregon). One of the things that you are unsure of is how the PEM keys on your Amazon Machine Images need to be migrated. Which of the following best describes how your PEM keys are affected when AMIs are migrated between regions? Choose the correct answer from the options below

- **A.** The PEM keys will also be copied across so you don't need to do anything except launch the new instance.
- **B.** The PEM keys will also be copied across; however, they will only work for users who have already accessed them in the old region. If you need new users to access the instances then new keys will need to be generated.
- **C.** Neither the PEM key nor the authorized key is copied and consequently you need to create new keys when you launch the new instance.
- **D.** The PEM keys will not be copied to the new region but the authorization keys will still be in the operating system of the AMI. You need to ensure when the new AMI is launched that it is launched with the same PEM key. ✔

Explanation :

Answer – D
Option A is incorrect because, as mentioned above, the PEM Keys are private keys and are never copied across the regions.
Option B is incorrect because the PEM keys are not user-specific.
Option C is incorrect because the authorization keys are copied across the region.
Option D is CORRECT because the authorization key is included in the AMI, hence copied across the region; however, the PEM keys are not copied; hence, need to be imported explicitly. See the AWS Console option for importing the PEM key.



For more information on EC2 key pairs, please visit the below URL

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

For more information on this subject, please visit the below forums on AWS

- https://forums.aws.amazon.com/thread.jspa?threadID=52654 (https://forums.aws.amazon.com/thread.jspa?threadID=52654)

Note:
You specify the name of the key pair when you launch an EC2 instance and provide the private key when you connect to that instance. Authorization Key here is the public key content (of the key pair) that is placed in an entry within **~/.ssh/authorized_keys** of that EC2 instance. This gets copied as part of the AMI.

Ask our Experts

QUESTION 76 UNATTEMPTED NETWORK DESIGN

You're working as a consultant for a company that has a three-tier application. The application layer of this architecture sends over 20Gbps of data per seconds during peak hours to and from Amazon S3. Currently, you're running two NAT gateways in two subnets to transfer the data from your private application layer to Amazon S3. You will also need to ensure that the instances receive software patches from a third party repository. What architecture changes should be made, if any? Choose the correct answer from the options below.

- **A.** NAT gateways support network performance of 10 Gbps and two of them are running: Add a third NAT Gateway to a separate subnet to allow for any increase in demand.
- **B.** Keep the NAT gateways and create a VPC S3 endpoint which allows for higher bandwidth throughput as well as tighter security ✔
- **C.** NAT gateways support 10Gbps and two are running: No changes are required to improve this architecture.
- **D.** Remove the NAT gateways and create a VPC S3 endpoint which allows for higher bandwidth throughput as well as tighter security.

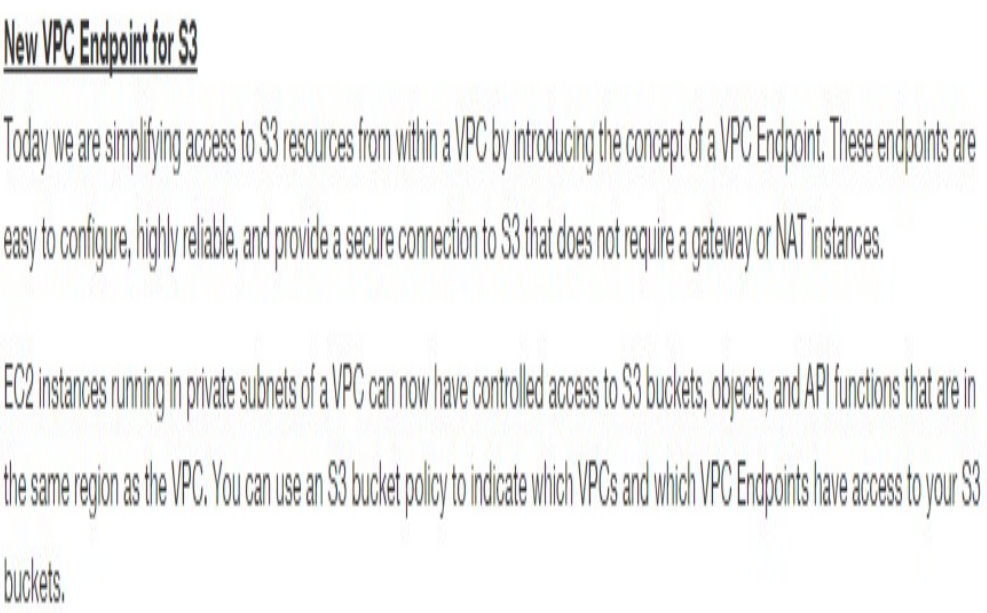
Explanation :

Answer – B

VPC Endpoints for Amazon S3 are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances. The EC2 instances running in a private subnets of a VPC can now have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.

Option A is incorrect because adding a third NAT Gateway for communicating with S3 bucket is a costly solution compared to creating an S3 endpoint.
Option B is CORRECT because (a) you can securely connect with S3 via the S3 endpoint, and (b) even though you can connect to S3 endpoint without requiring a NAT gateway, you still need to keep it because the instances in the VPC needs to receive the software patches from the third party repository. See the image in the *More information on VPC Endpoint for S3* section.
Option C is incorrect because you need to connect to the Amazon S3 via VPC endpoint as the current NAT gateways may not be sufficient to handle the peak load.
Option D is incorrect because if you remove the NAT Gateway, the instances in the VPC will not be able to receive the software patches from the third party repository.

More information on VPC Endpoint for S3
VPC endpoints alleviate the need for everything to go through the NAT instance
New VPC Endpoint for S3
Today we are simplifying access to S3 resources from within a VPC by introducing the concept of a VPC Endpoint. These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instances.
EC2 instances running in private subnets of a VPC can now have controlled access to S3 buckets, objects, and API functions that are in the same region as the VPC. You can use an S3 bucket policy to indicate which VPCs and which VPC Endpoints have access to your S3 buckets.



For more information on VPC endpoints please refer to the below URL:
https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/
(https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/)

Ask our Experts

QUESTION 77 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

BCJC is running Oracle DB workloads on AWS. Currently, they are running the Oracle RAC configuration on the AWS public cloud. You've been tasked with configuring backups on the RAC cluster to enable durability. What is the best method for configuring backups? Choose the correct answer from the options below

- **A.** Create manual snapshots of the RDS backup and write a script that runs the manual snapshot.
- **B.** Enable Multi-AZ failover on the RDS RAC cluster to reduce the RPO and RTO in the event of disaster or failure.
- **C.** Create a script that runs snapshots against the EBS volumes to create backups and durability. ✔
- **D.** Enable automated backups on the RDS RAC cluster; enable auto snapshot copy to a backup region to reduce RPO and RTO.

Explanation :

Answer – C
Currently, Oracle Real Application Cluster (RAC) is not supported as per the AWS documentation. However, you can deploy scalable RAC on Amazon EC2 using the recently-published tutorial (https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/)and Amazon Machine Images (AMI). So, in order to take the backups, you need to take the backup in the form of EBS volume snapshots of the EC2 that is deployed for RAC.

Option A, B, and D are all incorrect because RDS does not support Oracle RAC.
Option C is CORRECT because Oracle RAC is supported via the deployment using Amazon EC2. Hence, for the data backup, you can create a script that takes the snapshots of the EBS volumes.

For more information on Oracle RAC on AWS, please visit the below URL:
https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/ (https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/)
https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/ (https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/)
https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/ (https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/)

Ask our Experts

QUESTION 78 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have multiple EC2 instances in three availability zones (AZs), with a load balancer configured for your application. You observe that only one of those AZs is receiving all the traffic. How can you ensure that all the AZs receive balanced traffic? Choose two correct answers from the options below:

- [ ] **A.** Disable sticky sessions ✔
- [ ] **B.** Reduce the frequency of the health checks
- [ ] **C.** Enable cross zone load balancer ✔
- [ ] **D.** Amazon recommends to use two availability zone behind ELB

Explanation :

Answer – A, C

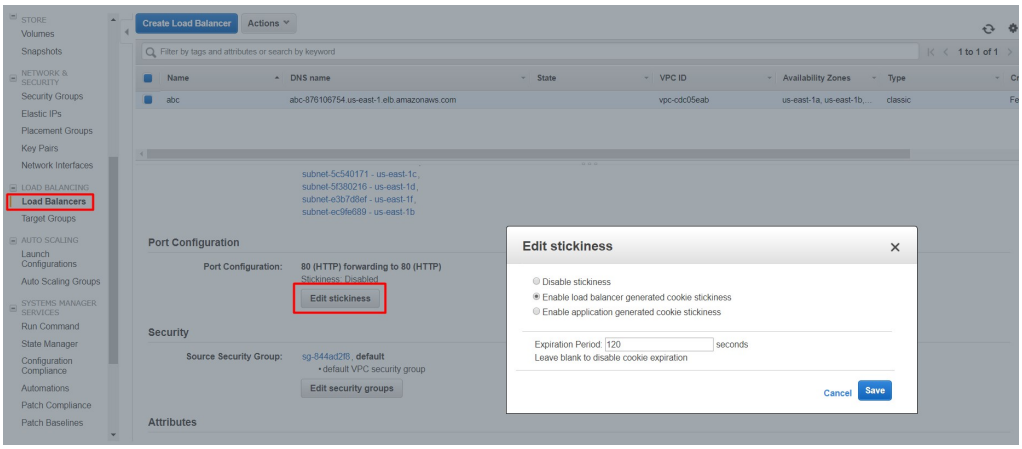
Since the traffic is routed to only one availability zone (AZ) and none of the other AZs are receiving any, the ELB must have only one AZ registered in it. First, you have to make sure that the ELB is configured to support multiple AZs via Cross-Zone load balancing. Even after enabling the cross zone load balancing, if the traffic is routed to particular EC2 instances in an AZ, the users' sessions must have tied to those EC2 instances. This symptoms seem to be related to the sticky sessions (session affinity). So, second thing you must ensure that the sticky sessions need to be either disabled or configured to be expiring after specific period.

Option A is CORRECT because, as mentioned above, sticky sessions could be a reason for traffic being

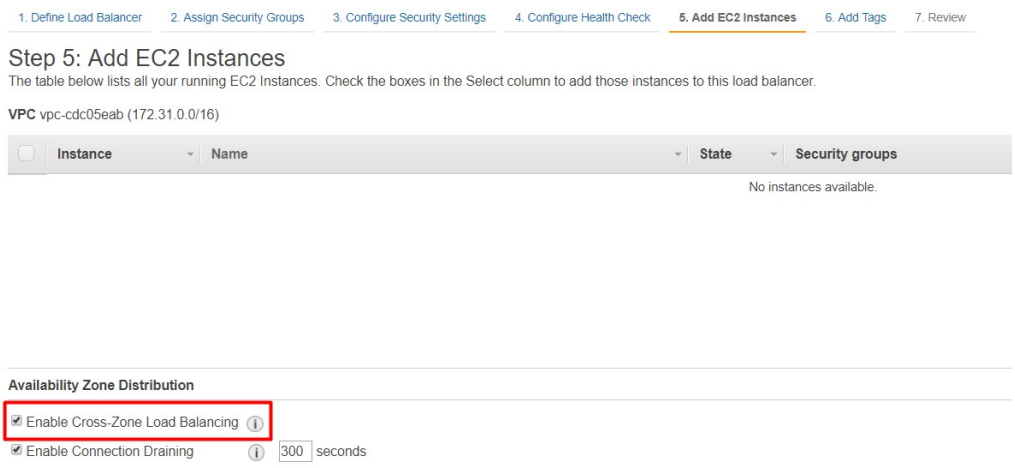
routed to specific EC2 instances in a specific AZ.
Option B is incorrect because reducing the health check frequency will not help in balancing the traffic between different AZs.
Option C is CORRECT because cross zone load balancing needs to be enabled on the ELB and the other AZs must be registered under this ELB.
Option D is incorrect because there is no such recommendation from Amazon about ELB.

More information on ELB, Sticky Sessions, and Cross Zone Load Balancing:

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html)



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 79 UNATTEMPTED NETWORK DESIGN

You are excited that your company has just purchased a Direct Connect link from AWS as everything you now do on AWS should be much faster and more reliable. Your company is based in Sydney, Australia so obviously, the Direct Connect Link to AWS will go into the Asia Pacific (Sydney) region. Your first job after the new link purchase is to create a multi-region design across the Asia Pacific(Sydney) region and the US West (N. California) region. You soon discover that all the infrastructure you deploy in the Asia Pacific(Sydney) region is extremely fast and reliable, however, the infrastructure you deploy in the US West(N. California) region is much slower and unreliable. Which of the following would be the best option to make the US West(N. California) region a more reliable connection? Choose the correct answer from the options below

- **A.** Create a private virtual interface to the Asia Pacific region's public end points and use VPN over the public virtual interface to protect the data.
- **B.** Create a private virtual interface to the US West region's public end points and use VPN over the public virtual interface to protect the data
- **C.** Create a public virtual interface to the Asia Pacific region's public end points and use VPN over the public virtual interface to protect the data.
- **D.** Create a public virtual interface to the US West region's public end points and use VPN over the public virtual interface to protect the data. ✔

Explanation :

Answer – D

AWS Direct Connect provides two types of virtual interfaces: public and private. To connect to AWS public endpoints, such as an Amazon Elastic Compute Cloud (Amazon EC2) or Amazon Simple Storage Service (Amazon S3), with dedicated network performance, use a public virtual interface. To connect to private services, such as an Amazon Virtual Private Cloud (Amazon VPC), with dedicated network performance, use a private virtual interface.

Since the scenario does not mention VPC only, you need to create a public virtual interface - which allows you to connect to all AWS public IP spaces globally.

Option A and B are incorrect because you need to create a public virtual interface to the US West region.
Option C is incorrect because you need to create a public virtual interface to the US West region - not Asia Pacific Region.
Option D is CORRECT because it creates a public virtual interface to the US West region which allows you to connect to the Asia Pacific region. Also, it uses secure VPN connection over the public virtual interface for the data protection.

For more information on virtual interfaces, please visit the below URLs:

- http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html (http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html)

- https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/ (https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/)
- https://aws.amazon.com/premiumsupport/knowledge-center/create-vpn-direct-connect/ (https://aws.amazon.com/premiumsupport/knowledge-center/create-vpn-direct-connect/)

Ask our Experts

QUESTION 80 UNATTEMPTED HIGH AVAILABILITY AND BUSINESS CONTINUITY

In Cloudfront, what is the Origin Protocol policy that must be chosen to ensure that the communication with the origin is done either via HTTP or HTTPS? Choose an answer from the options below

- A. HTTP
- B. HTTPS
- C. Match Viewer ✔
- D. None of the above

Explanation :

Answer – C

Options A, B, and D are all incorrect because the answer is Match Viewer.
Option C is CORRECT because if the Origin Protocol Policy is set to Match Viewer, the CloudFront communicates with the origin using HTTP or HTTPS depending upon the protocol of the viewer request.
AWS Document Says:
Origin Protocol Policy (Amazon EC2, Elastic Load Balancing, and Other Custom Origins Only)
The protocol policy that you want CloudFront to use when fetching objects from your origin server.
Important
If your Amazon S3 bucket is configured as a website endpoint, you must specify HTTP Only. Amazon S3 doesn't support HTTPS connections in that configuration.
Choose one of the following values:

- HTTP Only: CloudFront uses only HTTP to access the origin.
- HTTPS Only: CloudFront uses only HTTPS to access the origin.
- Match Viewer: CloudFront communicates with your origin using HTTP or HTTPS, depending on the protocol of the viewer request. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

Important
For HTTPS viewer requests that CloudFront forwards to this origin, one of the domain names in the SSL certificate on your origin server must match the domain name that you specify for Origin Domain Name. Otherwise, CloudFront responds to the viewer requests with an HTTP status code 502 (Bad

Gateway) instead of the requested object. For more information, see Requirements for Using SSL/TLS Certificates with CloudFront.
For more information on Cloudfront CDN please see the below link
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html (http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13603)

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)