

[Home](https://www.whizlabs.com/learn/) (<https://www.whizlabs.com/learn/>) > [My Courses](https://www.whizlabs.com/learn/my-courses) (<https://www.whizlabs.com/learn/my-courses>)> [AWS Certified Solutions Architect Professional](https://www.whizlabs.com/learn/course/aws-csap-practice-tests#section-1) (<https://www.whizlabs.com/learn/course/aws-csap-practice-tests#section-1>)> [Practice Test I](https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13604) (<https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13604>) > **Report**

PRACTICE TEST I

Attempt 1

Marks Obtained 0 / 80

Your score is 0.0%

Completed on Tuesday , 29 January 2019 , 01:34 PM

Time Taken 00 H 00 M 08 S

Result Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	High Availability and Business Continuity	14	0	1	13
2	Costing	13	0	0	13
3	Security	19	0	0	19
4	Deployment Management	10	0	0	10
5	Cloud Migration & Hybrid Architecture	10	0	0	10
6	Scalability & Elasticity	6	0	0	6
7	Data Storage	1	0	0	1
8	Network Design	7	0	0	7

80 Questions	0 Correct	1 Incorrect	79 Unattempted
------------------------	---------------------	-----------------------	--------------------------

Show Answers

All	▼
-----	---

QUESTION 1

INCORRECT

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company is hosting a web application on AWS. According to the architectural best practices, the application must be highly available, scalable, cost effective, with high-performance and should require minimal human intervention. You have deployed the web servers and database servers in public and private subnet of the VPC respectively. While testing the application via web browser, you noticed that the application is not accessible.

Which of the following two configuration settings can help you to tackle this issue?

Choose any two options where each one will provide an independent solution to tackle the issue.

- ☒ **A.** Configure a NAT instance in your VPC and create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address. ✕
- ☐ **B.** Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
- ☒ **C.** Place all your web servers behind ELB. Configure a Route53 ALIAS-Record to point to the ELB DNS name. ✓
- ☐ **D.** Assign EIP's to all web servers. Configure a Route53 A-Record set with all EIPs with health checks and DNS failover. ✓
- ☐ **E.** Configure ELB with an EIP. Place all your Web servers behind ELB. Configure a Route53 A record that points to the EIP.

Explanation :

Answers – C and D

- Option A is incorrect because (a) NAT instance is ideally used to route traffic from a private subnet to the internet via a public subnet, (b) NAT instance is not managed by AWS and requires to be

configured and maintained by the user; hence, adding to the overhead, and (c) if not scaled, can cause performance bottleneck. NAT Gateway is a preferred option over NAT instances.

- Option B is recommending us to use AWS CloudFront and configure the distributions Origin to the web server and then use a AWS Route 53 'CNAME' for the CloudFront Distribution. Even though CloudFront is highly available and is accessible to the Internet, it would work better if the Origin for the AWS CloudFront Distribution was pointed to an AWS ELB rather than to the Web Server itself.

Since the Origin would only be a Web Server, if this server goes offline for a period of time, the web site would become unavailable the content is not cached at the Edge location or if the TTL for the content expires.

So, Option B is incorrect as well.

- Option C is CORRECT. Because, (a) if the web servers are behind an ELB, the load on the web servers will be uniformly distributed. Hence, if any of the web servers goes offline or becomes non-responsive, the traffic would be routed to other online web servers; making the application highly available, and (b) You can use Route53 to set the ALIAS record that points to the ELB endpoint.

Create Record Set

Name: .awssampletest.com.

Type:

Alias: ☒ Yes ☐ No

Alias Target:

Alias Hosted Zone ID: Z35SXDOTRQ7X7K

You can also type the domain name for the resource. Examples:

- CloudFront distribution domain name: d1111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-1.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com

[Learn More](#)

Routing Policy:

Route 53 responds to queries based only on the values in this record. [Learn More](#)

- Option D is CORRECT. Because in Route53, you can either resolve the DNS query via creating an ALIAS record pointing to the ELB endpoint or an A record pointing to the IP Addresses of the application. As the EIPs are static (will not be changed) and can be assigned to new web servers if any of the web servers becomes offline, the EIPs can be used in the A record. The health check would ensure that Route53 checks the health of the record set before the failover to other web servers.

Create Record Set

Name:

www

.awssampletest.com.

Type:

A – IPv4 address

Alias:

☐ Yes ☒ No

TTL (Seconds):

300

1m

5m

1h

1d

Value:

52.70.113.126

54.173.104.79

34.226.150.123

IPv4 address. Enter multiple addresses on separate lines.

Example:

192.0.2.235

198.51.100.234

Routing Policy:

Failover

Route 53 responds to queries using primary record sets if any are healthy, or using secondary record sets otherwise. [Learn More](#)


Failover Record Type:

☒ Primary ☐ Secondary

Set ID:

www-Primary-1

Associate with Health Check:

☒ Yes ☐ No 

When responding to queries, Route 53 can omit resources that fail health checks. [Learn More](#)

Health Check to Associate:

HealthCheck

- Option E is incorrect because AWS does not recommend to assign IP Addresses to ELB. The public IP addresses get automatically assigned to the ELB's. You should always use the DNS name of the ELB.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html> (<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>)

<https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/> (<https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/>)

Ask our Experts



QUESTION 2

UNATTEMPTED

COSTING

You have developed an application that processes massive amount of process logs generated by web site and mobile app. This application requires the ability to analyze petabytes of unstructured data using Amazon Elastic MapReduce. The resultant data is stored on Amazon S3. You have deployed c4.8xlarge Instance type, whose CPUs are mostly idle during the data processing. Which of the below options would be the most cost-efficient way to reduce the runtime of the log processing job?

- ☐ A. Create log files with smaller size and store them on Amazon S3. Apply the life cycle policy to the S3 bucket such that the files would be first moved to RRS and then to Amazon Glacier vaults.
- ☐ B. Add additional c4.8xlarge instances by introducing a task instance group. The network performance of 10 Gigabit per EC2 instance would increase the processing speed; thus reducing the load on the EMR cluster.
- ☒ C. Use smaller instances that have higher aggregate I/O performance. ✓
- ☐ D. Create fewer, larger log files. Compress and store them on Amazon S3 bucket. Apply the life cycle policy to the S3 bucket such that the files would be first moved to RRS and then to Amazon Glacier vaults.

Explanation :

Answer – C

Option A is incorrect even though storing the files on S3 storage class such as RRS would reduce the cost. The problem in the scenario is that the provision of a large instance is wasted due to it being idle most of the time.

Option B is incorrect as adding more of c4.8xlarge instance type in the task instance group would create more idle resources, which is - in fact - more costly.

Option C is CORRECT because, since the CPU's are mostly idle, it means that you have provisioned a larger instance which is under-utilized. A better cost-efficient solution would be to use smaller instances. For batch processing jobs such as the one mentioned in this scenario, you can use multiple t2 instances - which support the concept of CPU bursts - are ideal for situations where there are bursts of CPU during certain periods of time only.

Option D is incorrect even though storing the files on S3 storage class such as RRS would reduce the cost. The problem in the scenario is that the provision of a large instance is wasted due to it being idle most of the time.

For more information on resizing of the EC2 instances, please visit the URL given below:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html>

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

Ask our Experts



QUESTION 3

UNATTEMPTED

COSTING

Your department creates regular analytics reports from your company's log files. All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse. You notice that the average EMR hourly usage is more than 25% but less than 50%.

Your CFO requests you to optimize the cost structure for this system. Which of the following alternatives will lower costs without compromising the average performance of the system or data integrity for the raw data?

- ☐ A. Use Glacier to store PDF and CSV Data. Add Spot instances to Amazon EMR jobs. Use Reserved instances for Amazon Redshift.
- ☐ B. Use standard S3 to store PDF. Use a combination of spot instances and reserved instances for EMR and reserved instances for RedShift. ✓
- ☐ C. Use Glacier to store PDF and CSV Data. Add Spot instances to Amazon EMR jobs. Use Spot instances for Amazon Redshift.

- ☐ D. Use S3-IA to store PDF and CSV Data. Use Reserved instances to Amazon EMR jobs. Use Reserved instances for Amazon Redshift.

Explanation :

Answer - B

Options A,C and D are invalid. We need to access the PDF and CSV files daily. So S3-IA and glacier are not suitable for this purpose as both of these storage options are not the best for frequent access of files.?

Ask our Experts



QUESTION 4

UNATTEMPTED

COSTING

You are the new IT architect in a company that operates a mobile sleep tracking application. When activated at night, the mobile app is sending collected data points of 1 KB every 5 minutes to your middleware. The middleware layer takes care of authenticating the user and writing the data points into an Amazon DynamoDB table. Every morning, you scan the table to extract and aggregate last night's data on a per-user basis, and store the results in Amazon S3. Users are notified via Amazon SMS mobile push notifications that new data is available, which is parsed and visualized by the mobile app. Currently, you have around 100k users. You have been tasked to optimize the architecture of the middleware system to lower the cost. What would you recommend?

Choose 2 options from below:

- ☐ A. Create a new Amazon DynamoDB table each day and drop the one for the previous day after its data is on Amazon S3. ✓
- ☐ B. Have the mobile app access Amazon DynamoDB directly instead of JSON files stored on Amazon S3.
- ☐ C. Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput. ✓

- ☐ D. . Introduce Amazon ElastiCache to cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.
- ☐ E. Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.

Explanation :

Answer – A and C

Option A is CORRECT because (a) The data stored would be old/obsolete anyways and need not be stored; hence, lowering the cost, and (b) Storing the data in DynamoDB is expensive; hence, you should not keep the tables with the data not needed.

Option B is incorrect because (a) Storing the data in DynamoDB is more expensive than S3, and (b) giving the app access to the DynamoDB to read the data is an operational overhead.

Option C is CORRECT because (a) it uses SQS which reduce the provisioned output cutting down on the costs, and (b) acts as a buffer that absorbs sudden higher load, eliminating going over the provisioned capacity.

Option D is incorrect because the data is only read once before its stored to S3. The cache would only be useful if you read things multiple times. Also, in this scenario optimizing "write" operations is most desired, not "read" ones.

Option E is incorrect because (a) Amazon Redshift cluster is primarily used for OLAP transactions, not OLTP; hence, not suitable for this scenario, and (b) moving the storage to Redshift cluster means deploying large number of EC2 instances that are continuously running, which is not a cost-effective solution.

For complete guidelines on working with DynamoDB, please visit the below URL:

<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GuidelinesForTables.html>
(<http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GuidelinesForTables.html>)

Ask our Experts



QUESTION 5

UNATTEMPTED

COSTING

Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high-resolution MP4 format. Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no

video transcoding expertise and it required you may need to pay for a consultant. How would you implement the most cost-efficient architecture without compromising high availability and quality of video delivery?

- ☒ **A.** Elastic Transcoder to transcode original high-resolution MP4 videos to HLS. Use S3 to host videos with Lifecycle Management to archive original files to Glacier after a few days. Use CloudFront to serve HLS transcoded videos from S3. ✓
- ☐ **B.** A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue. Use S3 to host videos with Lifecycle Management to archive all files to Glacier after a few days. Use CloudFront to serve HLS transcoding videos from Glacier.
- ☐ **C.** Elastic Transcoder to transcode original high-resolution MP4 videos to HLS EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days. CloudFront to serve HLS transcoded videos from EC2.
- ☐ **D.** A video transcoding pipeline running on EC2 using SQS to distribute tasks and Auto Scaling to adjust the number of nodes depending on the length of the queue EBS volumes to host videos and EBS snapshots to incrementally backup original files after a few days CloudFront to serve HLS transcoded videos from EC2.

Explanation :

Answer – A

There are four most important design considerations here: (a) video transcoding expertise, (b) global distribution of the content, (c) cost-effective solution, and (d) no compromise with the high availability and quality of the video delivery.

Amazon Elastic Transcoder is a media transcoding service in the cloud. It is designed to be a highly scalable, easy to use and a cost-effective way for developers and businesses to convert (or “transcode”) media files from their source format into versions that will playback on various devices like smartphones, tablets, and PCs.

- Option A is CORRECT because (a) it uses Amazon Elastic Transcoder that converts from MP4 to HLS, (b) S3 Object Lifecycle Management reduces the cost by archiving the files to Glacier, and (c) CloudFront - which is a highly available service - enables the global delivery of the video without compromising the video delivery speed or quality.

•

Option B is incorrect because (a) it necessitates the overhead of infrastructure provisioning. i.e deploying of EC2 instances, auto scaling, SQS queue / pipeline, (b) setting up of EC2 instances to handle global delivery of content is not a cost efficient solution.

•

Option C is incorrect because the use of EBS snapshots is not a cost effective solution compared to S3 Object Lifecycle Management.

- Option D is incorrect because (a) it necessitates the overhead of infrastructure provisioning. i.e deploying of EC2 instances, auto scaling, SQS queue / pipeline, (b) setting up of EC2 instances to handle global delivery of content is not a cost efficient solution, and (d) the use of EBS snapshots is not a cost effective solution compared to S3 Object Lifecycle Management.

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

- <https://aws.amazon.com/elastictranscoder/> (<https://aws.amazon.com/elastictranscoder/>)

Cloudfront can be then used to deliver the content to the users from its various edge locations.

Ask our Experts



QUESTION 6

UNATTEMPTED

COSTING

You've been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3. They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and a flood of superfluous requests for accessing the resources. You suspect that someone is attempting to gain unauthorized access. Which approach provides a cost-effective scalable mitigation to this kind of attack?

- ☐ A. Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC. Then they would establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF) and then pass the traffic through the DirectConnect connection into their application running in their VPC.
- ☐ B. Add previously identified host file source IPs as an explicit INBOUND DENY NACL to the web tier subnet.

- ☐ C. Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group ✓
- ☐ D. Remove all but TLS 1 & 2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Explanation :

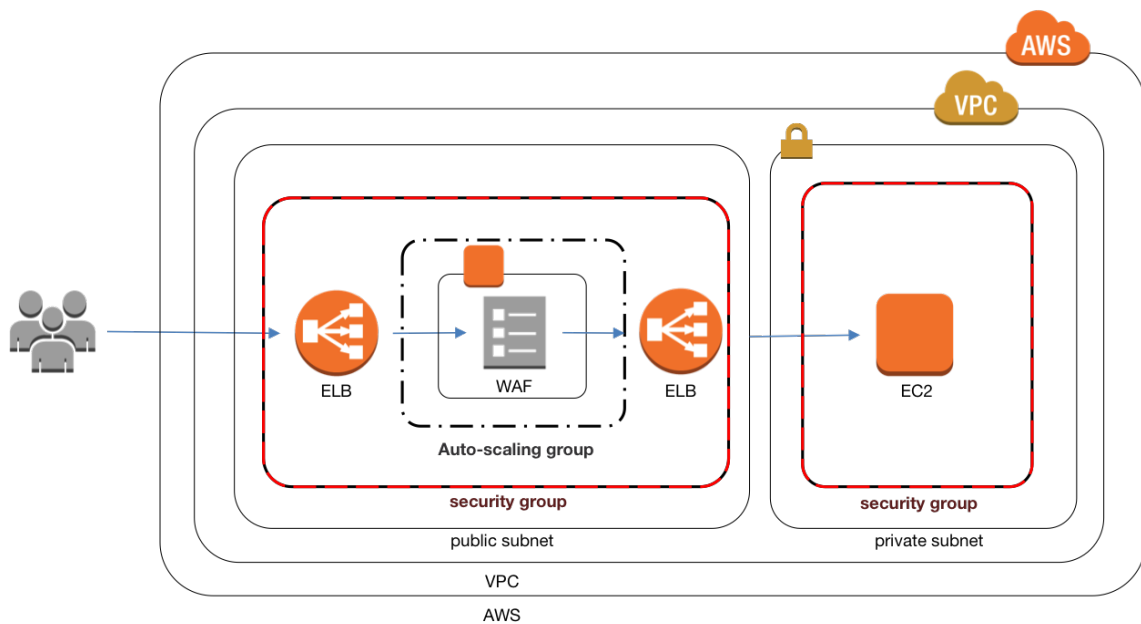
Answer – C

In such scenarios where you are designing a solution to prevent the DDoS attack (indicated by the flood of superfluous request for accessing the resources and suspicious activity) , always think of using Web Access Firewall (WAF).

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns.

Option A is incorrect because, although this option could work, the setup is very complex and it is not a cost effective solution.

Option B is incorrect because, (a) even though blocking certain IPs will mitigate the risk, the attacker could maneuver the IP address and circumvent the IP check by NACL, and (b) it does not prevent the attack from the new source of threat.



Option C is CORRECT because (a) WAF Tiers acts as the first line of defense, it filters out the known sources of attack and blocks common attack patterns, such as SQL injection or cross-site scripting, (b) the ELB of the application is not exposed to the attack, and most importantly (c) this pattern - known as "WAF Sandwich" pattern - has WAF layer with EC2 instances are placed between two ELBs - one that faces the web, receives all the traffic, and sends them to WAF layer to filter out the malicious requests, and sends the filtered non-malicious requests, another ELB - which receives the non-malicious requests and send them to the EC2 instances for processing. See the image below:

Option D is incorrect because there is no such thing as Advanced Protocol Filtering feature for ELB.

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

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

Ask our Experts



QUESTION 7

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You currently operate a web application in the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a

reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of the below solutions would you recommend?

- ☐ **A.** Create a new CloudTrail trail with one new S3 bucket to store the logs and with the option that applies trail to all regions selected. Use IAM roles, S3 bucket policies and Multi Factor Authentication (MFA) to delete on the S3 bucket that stores your logs. ✓
- ☐ **B.** Create a new CloudTrail with one new S3 bucket to store the logs. Configure SNS to send log file delivery notifications to your management system. Use IAM roles and S3 bucket policies on the S3 bucket that stores your logs.
- ☐ **C.** Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the option that applies trail to all regions selected. Use S3 ACLs and Multi Factor Authentication (MFA) to delete on the S3 bucket that stores your logs
- ☐ **D.** Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tools. Use IAM roles and S3 bucket policies on the S3 buckets that store your logs.

Explanation :

Answer – A

For the scenarios where the application is tracking (or needs to track) the changes made by any AWS service, resource, or API, always think about AWS CloudTrail service.

AWS Identity and Access Management (IAM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets.

The most important points in this question are (a) Use of a single S3 bucket, (b) CloudTrail with the option that applies trail to all regions enabled, (b) Data integrity, and (d) Confidentiality.

Option A is CORRECT because (a) it uses AWS CloudTrail with the option that applies trail to all regions enabled, (b) a single new S3 bucket and IAM Roles so that it has the confidentiality, (c) MFA on Delete on S3 bucket so that it maintains the data integrity. See the AWS CloudTrail setting below which sets the option that applies trail to all regions:

CloudTrail

Dashboard

Event history

Trails

Create Trail

Trail name*

CloudTrailForTest

Apply trail to all regions

☒ Yes ☐ No



Options B is incorrect because (a) although it uses AWS CloudTrail, the option that applies trail to all regions is not enabled, and (b) SNS notifications can be a overhead in this situation.

Option C is incorrect because (a) as an existing S3 bucket is used, it may already be accessed to the user, hence not maintaining the confidentiality, and (b) it is not using IAM roles.

Option D is incorrect because (a) although it uses AWS CloudTrail, the option that applies trail to all regions is not enabled, and (b) three S3 buckets are not needed.

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

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events>

(<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-global-service-events>)

<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>

(<http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>)

Ask our Experts



QUESTION 8

UNATTEMPTED

SECURITY

An enterprise wants to use a 3rd party SaaS application hosted by another AWS account. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account. The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party.

Which of the following options would meet all of these conditions?

- ☐ A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account
- ☐ B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application. Create a new access and secret key for the user and provide these credentials to the SaaS provider.
- ☐ C. Create an IAM role for cross-account access that allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application. ✓
- ☐ D. Create an IAM role for EC2 instances, assign it a policy which allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider, to be used when launching their application instances.

Explanation :

Answer – C

When a user, a resource, an application, or any service needs to access any AWS service or resource, always prefer creating appropriate role that has least privileged access or only required access, rather than using any other credentials such as keys.

- Option A is incorrect because you should never share your access and secret keys.
- Option B is incorrect because (a) when a user is created, even though it may have the appropriate policy attached to it, its security credentials are stored in the EC2 which can be compromised, and (b) creation of the appropriate role is always the better solution rather than creating a user.
- Option C is CORRECT because AWS role creation allows cross-account access to the application to access the necessary resources. See the image and explanation below:

Many SaaS platforms can access AWS resources via a Cross-account access created in AWS. If you go to Roles in your identity management, you will see the ability to add a cross-account role.

Select Role Type

☐ AWS Service Roles

☒ Role for Cross-Account Access

› Provide access between AWS accounts you own

Allows IAM users from one of your other AWS accounts to access this account.

› Provide access between your AWS account and a 3rd party AWS account

Allows IAM users from a 3rd party AWS account to access this account and enforces use of [External ID](#).

☐ Role for Identity Provider Access

- Option D is incorrect because the role is to be assigned to the application and its resources, not the EC2 instances.

For more information on the cross-account role, please visit the below URL:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

Ask our Experts



You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via the third party via their URLs. You want to explicitly deny any other outbound connections from your VPC instances to hosts on the internet.

Which of the following options would you consider?

- ☐ **A. Place all EC2 instances that do not require direct access to the internet in private subnets so their egress traffic can be directed to a web proxy server in public subnet and enforce URL based rules for outbound access. Remove default routes. ✓**
- ☐ **B. Implement security groups and configure outbound rules to only permit traffic to software depots.**
- ☐ **C. Move all your instances into private VPC subnets. Remove default routes from all routing tables and add specific routes to the software depots and distributions only.**
- ☐ **D. Implement network access control lists to allow traffic from specific destinations, with an implicit deny as a rule.**

Explanation :

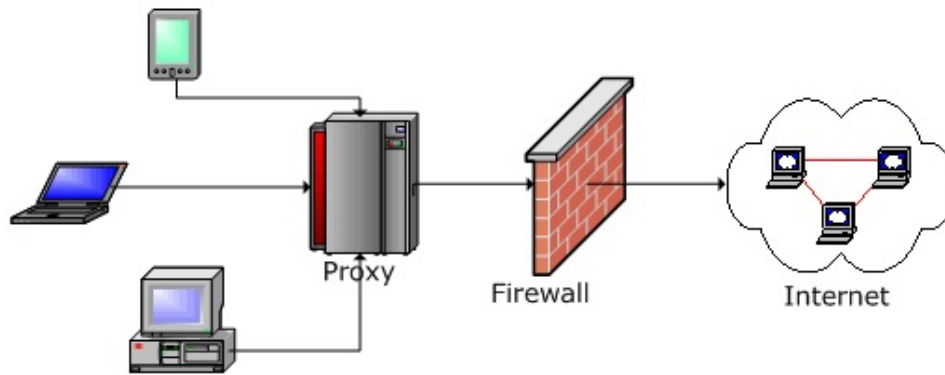
Answer - A

There are 3 main considerations in this scenario: (a) the instances in your VPC needs internet access, (b) the access should be restricted for product updates only, and (c) all other outbound connection requests must be denied.

With such scenarios, you should not put your instances in public subnet as they would have access to internet without any restrictions. So, you should put them in a private subnet, and since there is a need of a logic for filtering the requests from client machines, configure a proxy server.

What is a Proxy Server?

Proxy server is a server that acts as a mediator between client(s) that sends requests and server that receives the requests and replies back. If any client requires any resources, it connects to the proxy server, and the proxy server evaluates the request based on its filtering rules. If the requests are valid, it connects to the server which receives the request and replies back. The proxy server also maintains cache; i.e., if any subsequent requests from same or other clients are received, it returns the result from the cache, saving the trip to and from the server. Hence, proxy servers tend to improve the performance. See the diagram below:



- Option A is CORRECT because a proxy server (a) filters requests from the client, and allows only those that are related to the product updates, and (b) in this case helps filtering all other requests except the ones for the product updates.
- Option B is incorrect because a security group cannot filter request based on URLs and you cannot specify deny rules.
- Option C is incorrect because even though moving the instances in a private subnet is a good idea, the routing table does not have the filtering logic, it only connects the subnets with internet gateway. Since the instances are all in private subnet it cannot directly contact the internet for downloading the updates.
- Option D is incorrect. NACL are stateless. The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated. Option D is only specifying an Inbound rule. But for an Inbound rule it should specify the Source rather than destination.

An example of setting up a proxy server can be found via the below URL:

- <https://aws.amazon.com/articles/6463473546098546>
(<https://aws.amazon.com/articles/6463473546098546>)

Ask our Experts



An administrator is using Amazon CloudFormation to deploy a three-tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage. While creating the CloudFormation template which of the following would allow the application instance access to the DynamoDB tables without exposing API credentials?

- ☐ A. Create an Identity and Access Management Role that has the required permissions to read and write from the required DynamoDB table and associate the Role to the application instances by referencing an instance profile.
- ☐ B. Use the Parameter section in the Cloud Formation template to have the user input Access and Secret Keys from an already created IAM user that has the permissions required to read and write from the required DynamoDB table.
- ☐ C. Create an IAM Role that has the required permission to read and write from the required DynamoDB table, add the role to the instance profile and associate the instance profile with the application instance. ✓
- ☐ D. Create an identity and Access Management user in the CloudFormation template that has permissions to read and write from the required DynamoDB table, use the GetAtt function to retrieve the Access and secret keys and pass them to the application instance through user-data.

Explanation :

Answer – C

The scenario requires the instance to have access to DynamoDB tables without having to use the API credentials. In such scenarios, always think of creating IAM Roles rather than IAM Users.

Option A is incorrect because the IAM Role is not associated to the application by referencing an instance profile, it has to be used as an instance profile property.

Option B is incorrect because (a) you should never expose the Access and Secret Keys while accessing the AWS resources, and (b) using IAM Role is more secured way of accessing the resources than using IAM Users with security credentials.

Option C is CORRECT because (a) it uses IAM Role with the appropriate permissions to access the resource, and (b) it references that Role in the instance profile property of the application instance. See an example given below:

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "RootRole": {
      "Type": "AWS::IAM::Role",
      "Properties": {
        "AssumeRolePolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [ {
            "Effect": "Allow",
            "Principal": {
              "Service": [ "ec2.amazonaws.com" ]
            },
            "Action": [ "sts:AssumeRole" ]
          } ]
        },
        "Path": "/",
        "Policies": [ {
          "PolicyName": "root",
          "PolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [ {
              "Effect": "Allow",
              "Action": "*",
              "Resource": "*"
            } ]
          }
        } ]
      }
    },
    "RootInstanceProfile": {
      "Type": "AWS::IAM::InstanceProfile",
      "Properties": {
        "Path": "/",
        "Roles": [ {
          "Ref": "RootRole"
        } ]
      }
    }
  }
}

```

Option D is incorrect because (a) you should never expose the Access and Secret Keys while accessing the AWS resources, (b) using IAM Role is more secured way of accessing the resources than using IAM Users with security credentials.

For more information on granting access to AWS resources via EC2 instance profile property, please visit the below URL:

<https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/java-dg-roles.html>

(<https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/java-dg-roles.html>)

For more information on adding IAM roles in CloudFormation templates, please visit the below URL:

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-iam-role.html> (<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-iam-role.html>)



QUESTION 11

UNATTEMPTED

SECURITY

An AWS customer is deploying an application that is composed of an auto scaling group of EC2 Instances. The customer's security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique X.509 certificate that contains the specific instance ID. In addition, an X.509 certificate must be designed by the AWS Key Management Service (KMS) in order to be trusted for authentication.

Which of the following configurations will support these requirements?

- ☐ A. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure an Auto Scaling group to launch instances with this role. Have the instances bootstrap, get the certificate from Amazon S3 upon first boot.
- ☐ B. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group. Have the launched instances generate a certificate signature request with the instance's assigned instance-id to the AWS KMS for signature.
- ☐ C. Configure the AutoScaling group to send an SNS notification of the launch of a new instance to the AWS Certificate Manager. Create a signed certificate using AWS Certificate Manager (ACM). ✓
- ☐ D. Configure the launched instances to generate a new certificate upon first boot. Have the AWS KMS poll the Auto Scaling group for associated instances and send new instances a certificate signature (that contains the specific instance-id).

Explanation :

Answer – C

This scenario requires (a) a x.509 certificate per instance created in the auto scaling group, (b) the certificate should be unique that contains the instance id, and (c) this certificate should be generated by a key management service (authoritative service).

- Option A is incorrect because (a) storing the signed certificate in S3 is a bad idea as it will not be unique for each the instance id, and (b) S3 is not a key management service and does not generate such certificates.

- Option B is incorrect because you need to generate the instance id first before generating the certificate that will be unique for that instance id. Therefore, embedding a certificate in the image and then launching the instance will not be useful at all.
- Option C is CORRECT because (a) once the instance is launched in the auto scaling group, it notifies the key management service to generate a signed certificate, (b) the key management service is trusted, and (c) once the certificate is generated, it is directly sent to the newly created instance; hence, the workflow is logical.
- Option D is incorrect because (a) the onus is on the EC2 instances to generate the signed certificate, (b) the requirement is to use a key management service to generate the signed certificate, and (c) AWS KMS does not have any feature to 'poll' any service.

For more information on AWS KMS, please visit the below URL:

- <https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf>
(<https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf>)

Note:

Please remember

ACM and KMS work together.

Certificate manager (ACM) creates certificate and KMS helps to create public Key and a private key

To configure website or application at https protocol we need to apply these keys.

ACM Private Key Security

When you [request a public certificate](#), AWS Certificate Manager (ACM) generates a public/private key pair. For [imported certificates](#), you generate the key pair. The public key becomes part of the certificate. ACM stores the certificate and its corresponding private key, and uses AWS Key Management Service (AWS KMS) to help protect the private key. The process works like this:

1. The first time you request or import a certificate in an AWS region, ACM creates an AWS-managed customer master key (CMK) in AWS KMS with the alias **aws/acm**. This CMK is unique in each AWS account and each AWS region.
2. ACM uses this CMK to encrypt the certificate's private key. ACM stores only an encrypted version of the private key (ACM does not store the private key in plaintext form). ACM uses the same CMK to encrypt the private keys for all certificates in a specific AWS account and a specific AWS region.
3. When you associate the certificate with a service that is integrated with AWS Certificate Manager, ACM sends the certificate and the encrypted private key to the service. You also implicitly create a grant in AWS KMS that allows the service to use the CMK in AWS KMS to decrypt the certificate's private key. For more information about grants, see [Using Grants](#) in the *AWS Key Management Service Developer Guide*. For more information about services supported by ACM, see [Services Integrated with AWS Certificate Manager](#).
4. Integrated services use the CMK in AWS KMS to decrypt the private key. Then the service uses the certificate and the decrypted (plaintext) private key to establish secure communication channels (SSL/TLS sessions) with its clients.
5. When the certificate is disassociated from an integrated service, the grant created in step 3 is retired. This means the service can no longer use the CMK in AWS KMS to decrypt the certificate's private key.

Please check below AWS Docs for more details:

- <https://docs.aws.amazon.com/acm/latest/userguide/kms.html>
(<https://docs.aws.amazon.com/acm/latest/userguide/kms.html>)

Ask our Experts



QUESTION 12

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

You are given a task with moving a legacy application from a virtual machine running inside your datacenter to an Amazon VPC. Unfortunately, this app requires access to a number of on-premise services and no one who configured the app still works for your company. Even worse, there's no documentation for it. What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured?

Choose 3 options the below:

- ☐ A. An AWS Direct Connect link between the VPC and the network housing the internal services. ✓
- ☐ B. An Internet Gateway to allow a VPN connection.
- ☐ C. An Elastic IP address on the VPC instance
- ☐ D. An IP address space that does not conflict with the one on-premises ✓
- ☐ E. Entries in Amazon Route 53 that allow the Instance to resolve its dependencies' IP addresses
- ☐ F. A VM Import of the current virtual machine. ✓

Explanation :

Answer: A, D and F

The scenario requires you to connect your on-premise server/instance with Amazon VPC. When such scenarios are presented, always think about services such as Direct Connect, VPN, and VM Import and Export as they help either connecting the instances from different location or importing them from one location to another.

- Option A is CORRECT because Direct Connect sets up a dedicated connection between on-premise data-center and Amazon VPC, and provides you with the ability to connect your on-premise servers with the instances in your VPC.

- Option B is incorrect as you normally create a VPN connection based off of a customer gateway and a virtual private gateway (VPG) in AWS.
- Option C is incorrect as EIPs are not needed as the instances in the VPC can communicate with on-premise servers via their private IP address.
- Option D is CORRECT because, there should not be a conflict between IP address of on-premise servers and the instances in VPC for them to communicate.
- Option E is incorrect because, Route53 is not useful in resolving on-premise dependency.
- Option F is CORRECT because VM Import Export service helps you to import the virtual machine images from the data center to AWS platform as EC2 instances and export them back to your on-premises environment. This offering allows you to leverage your existing investments in the virtual machines that you have built to meet your IT security, configuration management, and compliance requirements by bringing those virtual machines into Amazon EC2 as ready-to-use instances.

Note:

Question doesn't mention that instances are in VPC, rather it asks for how to migrate virtual machines on premise to VPC in last sentence of the question.

VMWare import can help us moving machines from on premise to ec2 instances inside VPC.

Recently there is an announcement from AWS regarding Route53 Support for resolving on premise dependency:

- <https://aws.amazon.com/about-aws/whats-new/2018/11/amazon-route-53-announces-resolver-with-support-for-dns-resolution-over-direct-connect-and-vpn/>
(<https://aws.amazon.com/about-aws/whats-new/2018/11/amazon-route-53-announces-resolver-with-support-for-dns-resolution-over-direct-connect-and-vpn/>)

As you are aware that latest features/announcements takes around 6 months to get reflected in the actual exam.

Ask our Experts



QUESTION 13

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

Your company has recently extended its data center into a VPC on AWS to add burst computing capacity as needed. Members of your Network Operations Center need to be able to go to the AWS Management Console and administer

Amazon EC2 instances as necessary. You don't want to create new IAM users for each member and make those users sign in again to the AWS Management Console. Which option below will meet the needs of your NOC members?

- ☐ A. Use OAuth 2.0 to retrieve temporary AWS security credentials to enable your members to sign in to the AWS Management Console.
- ☐ B. Use web Identity Federation to retrieve AWS temporary security credentials to enable your members to sign in to the AWS Management Console.
- ☐ C. Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint ✓
- ☐ D. Use your on-premises SAML 2.0-compliant identity provider (IDP) to retrieve temporary security credentials to enable members to sign in to the AWS Management Console.

Explanation :

Answer – C

This scenario has two requirements: (a) temporary access to AWS resources be given to certain users or application (NOC members in this case), and (b) you are not supposed to create new IAM users for the NOC members to log into AWS console.

This scenario is handled by a concept named "Federated Access". Read this for more information on federated access: <https://aws.amazon.com/identity/federation/> (<https://aws.amazon.com/identity/federation/>).

Read this article for more information on how to establish the federated access to the AWS resources:

<https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-active-directory-user-attributes/> (<https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-active-directory-user-attributes/>)

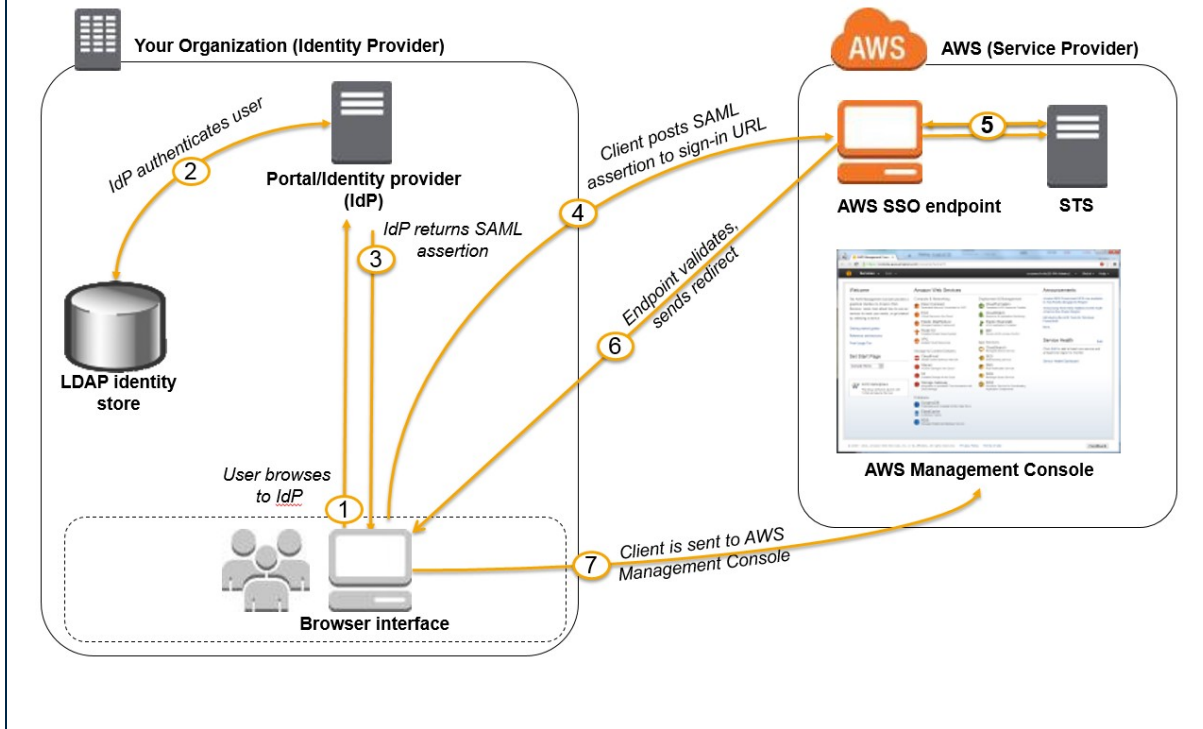
Option A is incorrect because OAuth 2.0 is not applicable in this scenario as we are not using Web Identity Federation as it is used with public identity providers such as Facebook, Google etc.

Option B is incorrect because the key point here is that you need to give access to AWS Management Console to only the members of your Network Operations Center using on premises SSO to avoid signing in again. The users should not be using Facebook or Google IDs to login.

Option C is CORRECT because (a) it gives a federated access to the NOC members to AWS resources by using SAML 2.0 identity provider, and (b) it uses on-premise single sign on (SSO) endpoint to authenticate users and gives them access tokens prior to providing the federated access.

Option D is incorrect because, even though it uses SAML 2.0 identity provider, one of the requirements is not to let users sign in to AWS console using any security credentials.

See this diagram that explains the Federated Access using SAML 2.0.



Ask our Experts



QUESTION 14

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient. Which of the following options would you consider for configuring the web server infrastructure?

Choose any 2 options from the list given below, each one being an independent solution to the scenario.

- ☐ A. Configure ELB with TCP listeners on TCP/443 and place the Web servers behind it. ✓
- ☐ B. Configure your Web servers with EIP's. Place the Web servers in a Route53 Record Set and configure health checks against all Web servers. ✓
- ☐ C. Configure ELB with HTTPS listeners, and place the Web servers behind it.
- ☐ D. Configure your web servers as the origins for a CloudFront distribution. Use custom SSL certificates on your CloudFront distribution.

Explanation :

Answers are A and B

This scenario requires you to setup the web servers in such a way that the HTTPS clients must be authenticated by the client-side certificate (not the server side certificate). There are two ways of architecting this - with ELB and without ELB. (a) With ELB, if you use HTTPS listener, you have to deploy the server side certificate - which is not desired. So, you need to use the TCP listener so that the HTTPS client requests do not terminate at the ELB, they just pass through ELB and terminate at the web server instances. (b) Alternatively, without ELB, you can directly use the web server to communicate with the clients, or set up a Route53 Record Set with the public IP address of the web server(s) such that the client requests would be directly routed to the web server(s).

Option A is CORRECT because it uses the TCP (443) listener so that the HTTPS client requests do not terminate at the ELB, they just pass through the ELB and terminate at the web server instances.

Option B is CORRECT because it uses Route53 Record Set with the public IP address of the web server(s) such that the client requests would be directly routed to the web server(s).

Option C is incorrect because if you use HTTPS listener, you must deploy an SSL/TLS certificate on your load balancer, i.e. authentication via the client certificate is not currently supported.

Option D is incorrect because this setting is currently not supported.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ssl-server-cert.html>
(<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ssl-server-cert.html>)
<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html#create-https-lb-console>
(<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html#create-https-lb-console>)

Ask our Experts



QUESTION 15

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your servers on-premises will be communicating with your VPC instances. You will be establishing IPSec tunnels over the internet. You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways.

Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above?

Choose 4 answers from the below:

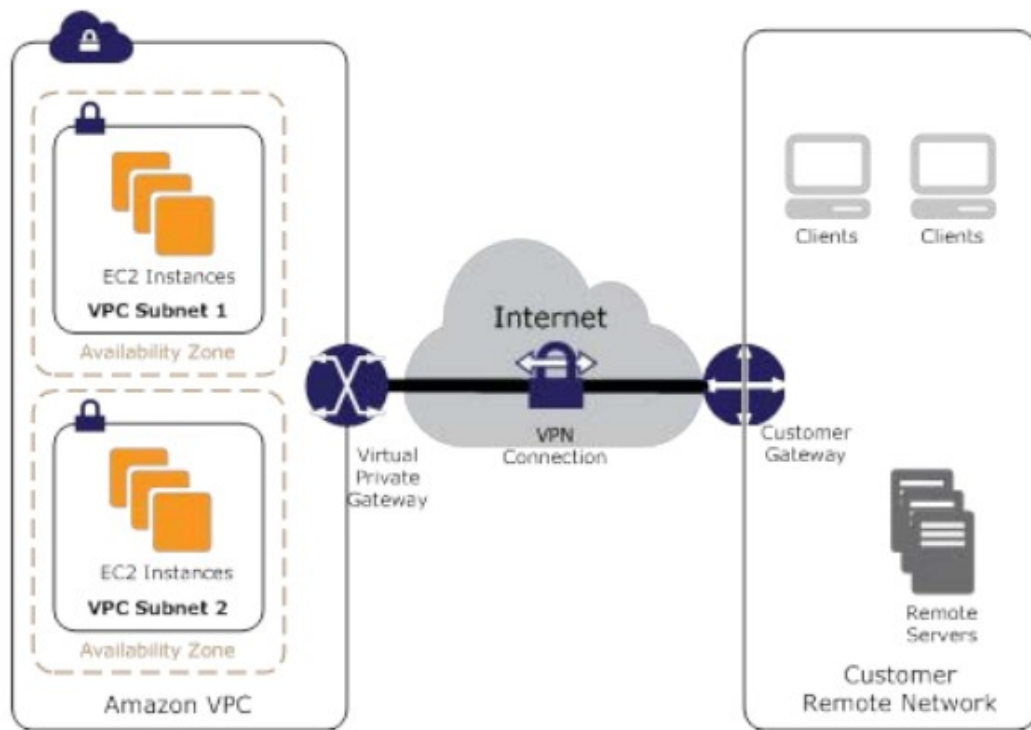
- ☐ A. End-to-end protection of data in transit
- ☐ B. End-to-end Identity authentication
- ☐ C. Data encryption across the Internet ✓
- ☐ D. Protection of data in transit over the Internet ✓
- ☐ E. Peer identity authentication between VPN gateway and customer gateway is achieved as it is imperative for its implementation. ✓
- ☐ F. Data integrity protection across the Internet ✓

Explanation :

Answer – C, D, E and F

IPSec is designed to provide authentication, integrity, and confidentiality of the data that is being transmitted. IPSec operates at network layer of the OSI model. Hence, it only protects the data that is in transit over the internet. For the full security of the data transmission it is very essential that both the sender and receiver need to be IPSec-aware.

See the diagram of this scenario:



AWS managed VPN

Option A is incorrect because (a) IPSec operates at network layer of the OSI model. Hence, it only protects the data that is in transit over the internet, and (b) both the source and the destination (client and server) may not be IPSec aware.

Option B is incorrect because the identity authentication of the origin of the data has to be done at the application layer, not the network layer.

Option C is CORRECT because the data that is transiting via the IPSec tunnel is encrypted.

Option D is CORRECT because IPSec protects the data that is in transit over the internet (fundamental responsibility of IPSec tunnel).

Option E is CORRECT because in this scenario, it is a pre-requisite to have the Peer identity authentication between VPN gateway and customer gateway for implementing IPSec VPN tunnel. The IPSec tunnel is established between VPN gateway (VPG) and Customer Gateway (CGW) whose identity gets authenticated during the setup of the IPSec tunnel.

Since it is a pre-requisite even for establishing this connection we cannot term that as an objective that we have achieved via the implementation of IPSec.

Option F is CORRECT because - as mentioned earlier - integrity of the data that is transiting via the IPSec tunnel is always preserved (fundamental responsibility of IPSec tunnel).

For more information on IPSec tunnel, please refer to:

http://techgenix.com/securing_data_in_transit_with_ipsec/

(http://techgenix.com/securing_data_in_transit_with_ipsec/)

The below link provides an article on the general working of an IPSec tunnel which outlines the advantages of an IPSec tunnel which includes:

<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>

(<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>)

Ask our Experts



QUESTION 16

UNATTEMPTED

SECURITY

You are designing an intrusion detection prevention (IDS/IPS) solution for a customer's web application in a single VPC. You are considering the options for implementing IDS/IPS protection for traffic coming from the Internet. Which of the following options would you consider?

Choose 2 options from the below

- ☐ A. Implement IDS/IPS agents on each Instance running In VPC ✓
- ☐ B. Configure an instance in each subnet to switch its network interface card to promiscuous mode and analyze network traffic.
- ☐ C. Implement Elastic Load Balancing with SSL listeners In front of the web applications
- ☐ D. Implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on each reverse proxy server. ✓

Explanation :

Answer – A and D

The main responsibility of Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) is to (a) detect the vulnerabilities in your EC2 instances, (b) protect your EC2 instances from attacks, and (c) respond to intrusion or attacks against your EC2 instances.

The IDS is an appliance that is installed on the EC2 instances that continuously monitors the VPC environment to see if any malicious activity is happening and alerts the system administration if such activity is detected. IPS, on the other hand, is an appliance that is installed on the EC2 instances that monitors and analyzes the incoming and outgoing network traffic for any malicious activities and prevents the malicious requests from reaching to the instances in the VPC.

This scenario is asking you how you can setup IDS/IPS in your VPC. There are few well known ways: (a) install the IDS/IPS agents on the EC2 instances of the VPC, so that the activities of that instance can be monitored, (b) set up IDS/IPS on a proxy server/NAT through which the network traffic is flowing, or (c) setup a Security-VPC that contains EC2 instances with IDS/IPS capability and peer that VPC with your VPC and always accept the traffic from Security-VPC only.

Option A is CORRECT because it implements the IDS/IPS agents on each EC2 instances in the VPC.

Option B is incorrect because promiscuous mode is not supported by AWS.

Option C is incorrect because ELB with SSL does not have the intrusion detection/prevention capability.

Option D is CORRECT because a reverse proxy server through which the traffic from instances inside VPC flows outside of it, has the IDS/IPS agent installed.

For more information on intrusion detection systems in AWS, please refer to the below link:

<https://awsmedia.s3.amazonaws.com/SEC402.pdf>

(<https://awsmedia.s3.amazonaws.com/SEC402.pdf>)

Ask our Experts



QUESTION 17

UNATTEMPTED

SECURITY

You are designing a photo-sharing mobile app. The application will store all pictures in a single Amazon S3 bucket. Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3. You want to configure security to handle potentially millions of users in the most secure manner possible.

What should be done by your server-side application, when a new user registers on the photo-sharing mobile application?

- ☐ A. Create a set of long-term credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app and use them to access Amazon S3.
- ☐ B. Record the user's Information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app create temporary credentials using the AWS Security Token Service 'AssumeRole' function, store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app. ✓

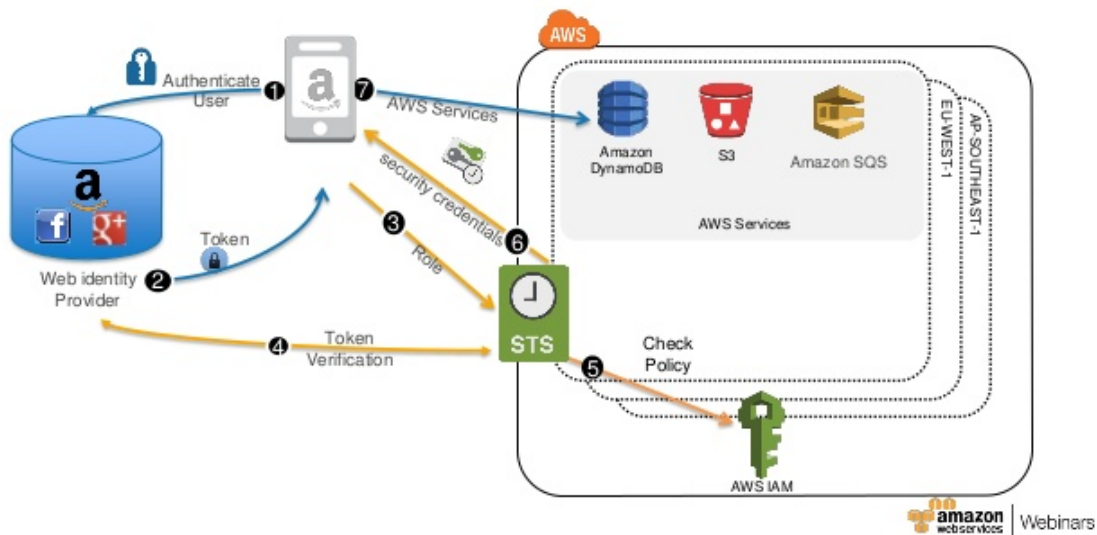
- C. Record the user's Information In Amazon DynamoDB. When the user uses their mobile app create temporary credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
- D. Create IAM user. Assign appropriate permissions to the IAM user Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
- E. Create an IAM user. Update the bucket policy with appropriate permissions for the IAM user. Generate an access Key and secret Key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.

Explanation :

Answer – B

This scenario requires the mobile application to have access to S3 bucket. There are potentially millions of users and a proper security measure should be taken. In such question, where mobile applications needs to access AWS Resources, always think about using functions such as "AssumeRole", "AssumeRoleWithSAML", and "AssumeRoleWithWebIdentity". See the following diagram that explains the flow of actions while using "AssumeRole".

Web Identity Federation (AssumeRoleWithWebIdentity)



You can let users sign in using a well-known third-party identity provider such as login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) 2.0 compatible provider. You can exchange the credentials from that provider for temporary permissions to use resources in your AWS account. This is known as the *web identity federation* approach to temporary access. When you use web identity federation for your mobile or web application, you don't need to create custom sign-in code or manage your own user identities. Using web identity federation helps you keep your AWS account secure because you don't have to distribute long-term security credentials, such as IAM user access keys, with your application.

Option A is incorrect because you should always grant the short term or temporary credentials for the mobile application. This option asks to create a long term credentials.

Option B is CORRECT because (a) it creates an IAM Role with appropriate permissions, (b) it generates temporary security credentials using STS "AssumeRole" function, and (c) it generates new credentials when the user runs the app the next time.

Option C is incorrect because, even though the set up is very similar to option B, it does not create IAM Role with proper permissions which is an essential step.

Option D is incorrect because, it asks to create an IAM User, not the IAM Role - which is not a good solution. You should create a IAM Role so that the app can access the AWS Resource via "AssumeRole" function.

Option E is incorrect because, it asks to create an IAM User, not the IAM Role - which is not a good solution. You should create a IAM Role so that the app can access the AWS Resource via "AssumeRole" function.

For more information on AWS temporary credentials, please refer to the below link:

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

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

https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html

(https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html)

Ask our Experts



QUESTION 18

UNATTEMPTED

SECURITY

You have an application running on an EC2 Instance which will allow users to download files from a private S3 bucket using a pre-signed URL. Before generating the URL, the application should verify the existence of the file in S3. How should the application use AWS credentials to access the S3 bucket securely?

- ☐ A. Use the AWS account access Keys. The application retrieves the credentials from the source code of the application.
- ☐ B. Create an IAM user for the application with permissions that allow list access to the S3 bucket launch the instance as the IAM user and retrieve the IAM user's credentials from the EC2 instance user data.
- ☐ C. Create an IAM role for EC2 that allows list access to objects in the S3 bucket. Launch the instance with the role, and retrieve the role's credentials from the EC2 Instance metadata ✓
- ☐ D. Create an IAM user for the application with permissions that allow list access to the S3 bucket. The application retrieves the IAM user credentials from a temporary directory with permissions that allow read access only to the application user.

Explanation :

Answer - C

An IAM *role* is similar to a user. In that, it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have any credentials (password or access keys) associated with it. Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources.

Whenever the question presents you with a scenario where an application, user, or service wants to access another service, always prefer creating IAM Role over IAM User. The reason being that when an IAM User is created for the application, it has to use the security credentials such as access key and secret key to use the AWS resource/service. This has security concerns. Whereas, when an IAM Role is created, it has all the necessary policies attached to it. So, the use of access key and secret key is not needed. This is the preferred approach.

Option A is incorrect because you should not use the account access keys , instead you should use the IAM Role.

Option B is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above.

Option C is CORRECT because, (a) it creates the IAM Role with appropriate permissions, and (b) the application accesses the AWS Resource using that role.

Option D is incorrect because instead of IAM User, you should use the IAM Role. See the explanation given above.

For more information on IAM roles, please visit 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 19

UNATTEMPTED

SECURITY

You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks. Which of the below are viable mitigation techniques?

Choose 3 options from the below

- ☐ A. Add multiple elastic network interfaces (ENIs) to each EC2 instance to increase the network bandwidth.
- ☐ B. Use dedicated instances to ensure that each instance has the maximum performance possible.
- ☐ C. Use an Amazon CloudFront distribution for both static and dynamic content. ✓
- ☐ D. Use an Elastic Load Balancer with auto scaling groups at the web, App. Restricting direct internet traffic to Amazon Relational Database Service (RDS) tiers. ✓
- ☐ E. Add alert Amazon CloudWatch to look for high network in and CPU utilization. ✓
- ☐ F. Create processes and capabilities to quickly add and remove rules to the instance OS firewall.

Explanation :

Answer – C, D, and E

This question is asking you to select some of the most recommended and widely used DDoS mitigation techniques.

What is a DDoS Attack?

A Distributed Denial of Service (DDoS) attack is an attack orchestrated by distributed multiple sources that makes your web application unresponsive and unavailable for the end users.

DDoS Mitigation Techniques

Some of the recommended techniques for mitigating the DDoS attacks are

- (i) build the architecture using the AWS services and offerings that have the capabilities to protect the application from such attacks. e.g. CloudFront, WAF, Autoscaling, Route53, VPC etc.
- (ii) defend the infrastructure layer by over-provisioning capacity, and deploying DDoS mitigation systems.
- (iii) defend the application layer by using WAF, and operating at scale by using autoscale so that the application can withstand the attack by scaling and absorbing the traffic.
- (iv) minimizing the surface area of attack
- (v) obfuscating the AWS resources

Option A is incorrect because ENIs do not help in increasing the network bandwidth.

Option B is incorrect because having dedicated instances performing at maximum capacity will not help mitigating the DDoS attack. What is needed is instances behind auto-scaling so that the traffic can be absorbed while actions are being taken on the attack and the application can continue responding to the clients.

Option C is CORRECT because (a) CloudFront is AWS managed service and it can scale automatically, (b) helps absorbing the traffic, and (c) it can help putting restriction based on geolocation. i.e. if the attack is coming from IPs from specific location, such requests can be blocked.

Option D is CORRECT because (a) ELB helps distributing the traffic to the instances that are part of auto-scaling (helps absorbing the traffic), and (b) Amazon RDS is an Amazon managed service which can withstand the DDoS attack.

Option E is CORRECT because CloudWatch can help monitoring the network traffic as well as CPU Utilization for suspicious activities.

Option F is incorrect because adding and removing rules of firewall is not going to mitigate the DDoS attack.

It is very important to read the AWS Whitepaper on Best Practices for DDoS Resiliency.

https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

(https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf)

Ask our Experts



QUESTION 20

UNATTEMPTED

SECURITY

A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload for the new fiscal year benefit enrollment period plus some extra overhead.

Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools. It is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrolment administrators cannot even SSH into them. Which activity would be useful in defending against this attack?

- ☐ A. Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
- ☐ B. Change the EIP (Elastic IP Address) of the NAT instance in the web tier subnet and update the Main Route Table with the new EIP
- ☐ C. Create 15 Security Group rules to block the attacking IP addresses over port 80
- ☐ D. Create an inbound NACL (Network Access control list) associated with the web tier subnet with deny rules to block the attacking IP addresses ✓

Explanation :

Answer – D

In this scenario, the attack is coming from a set of certain IP addresses over specific port from a specific country. You are supposed to defend against this attack.

In such questions, always think about two options: Security groups and Network Access Control List (NACL). Security Groups operate at the individual instance level, whereas NACL operates at subnet level. You should always fortify the NACL first, as it is encountered first during the communication with the instances in the VPC.

Option A is incorrect because IP addresses cannot be blocked using route table or IGW.

Option B is incorrect because changing the EIP of NAT instance cannot block the incoming traffic from a particular IP address.

Option C is incorrect because (a) you cannot deny port access using security groups, and (b) by default all requests are denied; you open access for particular IP address or range. You cannot deny access for particular IP addresses using security groups.

Option D is CORRECT because (a) you can add deny rules in NACL and block access to certain IP addresses. See an example below:

Summary

Inbound Rules

Outbound Rules

Subnet Associations

Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
150	NFS (2049)	TCP (6)	2049	54.209.0.0/16	DENY
200	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html
[\(https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html\)](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html)

Ask our Experts

QUESTION 21

UNATTEMPTED

SECURITY

Your fortune 500 company has undertaken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware. The outcome was that all employees would be granted access to use Amazon S3 for storage of their personal documents. Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket?

Choose 3 options from the below

- ☐ A. Setting up a federation proxy or identity provider ✓
- ☐ B. Using AWS Security Token Service to generate temporary tokens ✓
- ☐ C. Tagging each folder in the bucket
- ☐ D. Configuring IAM role ✓

- ☐ E. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket

Explanation :

Answer – A, B, and D

In questions like this where an application, or user needs to be given access using Single Sign On (SSO), following steps are very important:

- (i) setting up a identity provider for federated access
- (ii) authenticating users using corporate data store / active directory-user-attributes/
- (iii) getting temporary access tokens / credentials using AWS STS
- (iv) creating the IAM Role that has the access to the needed AWS Resources

Option A is CORRECT because as mentioned above, setting up a identity provider for federated access is needed.

Option B is CORRECT because as mentioned above, getting temporary access tokens / credentials using AWS STS is needed.

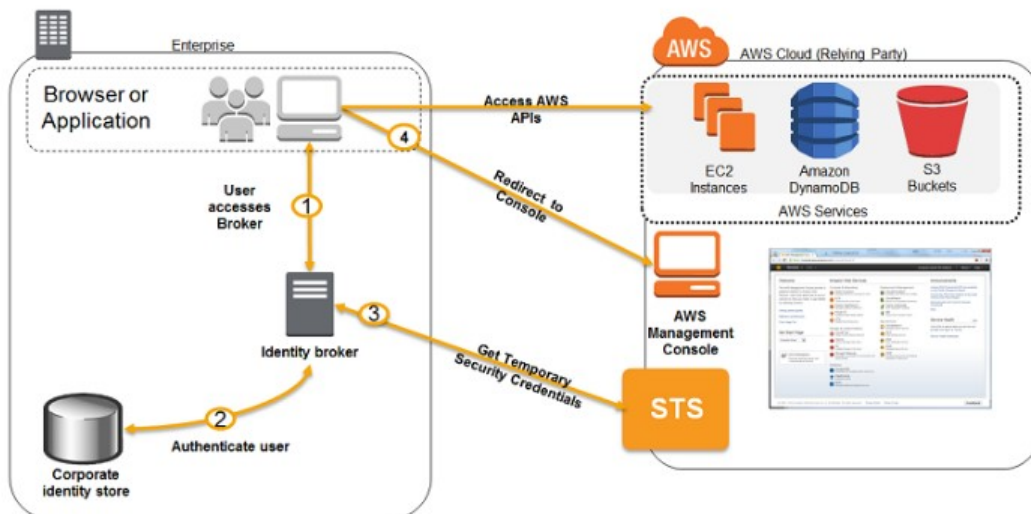
Option C is incorrect because tagging each folder in bucket does not help in this scenario.

Option D is CORRECT because as mentioned above, creating the IAM Role that has the access to the needed AWS Resources is needed.

Option E is incorrect because you should be creating IAM Roles rather than IAM Users.

The diagram below showcases how authentication is carried out when having an identity broker.

This is an example of a SAML connection , but the same concept holds true for getting access to an AWS resource.



For more information on federated access, please visit the below link:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html)

Ask our Experts



QUESTION 22

UNATTEMPTED

SECURITY

Your company policies require encryption of sensitive data at rest. You are considering the possible options for protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance. Which of these options would allow you to encrypt your data at rest?

Choose 3 options from the below

- ☐ A. Implement third party volume encryption tools ✓
- ☐ B. Do nothing as EBS volumes are encrypted by default
- ☐ C. Encrypt data inside your applications before storing it on EBS ✓
- ☐ D. Encrypt data using native data encryption drivers at the file system level ✓
- ☐ E. Implement SSL/TLS for all services running on the server

Explanation :

Answer – A, C, and D

You can encrypt the data at rest by either using a native data encryption, using a third party encrypting tool, or just encrypt the data before storing on the volume.

Option A CORRECT because it uses third party volume encryption tool.

Option B is incorrect because EBS volumes are not encrypted by default.

Option C is CORRECT as it encrypts the data before storing it on EBS.

Option D is CORRECT as it uses the native data encryption.

Option E is incorrect as SSL/TLS is used for the security of the data in transit, not at rest.

Ask our Experts



You are migrating a legacy client-server application to AWS. The application responds to a specific DNS domain (e.g. `www.example.com`) and has a 2-tier architecture, with multiple application servers and a database server. Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket. A decision is made to use multi-AZ RDS MySQL instance for the database. During the migration, you can change the application code but you have to file a change request.

How would you implement the architecture on AWS In order to maximize scalability and high-availability?

- ☐ A. File a change request to implement Proxy Protocol Support. In the application use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two application servers in different AZs. ✓
- ☐ B. File a change request to Implement Cross-Zone support in the application Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
- ☐ C. File a change request to implement Latency Based Routing support in the application. Use Route 53 with Latency Based Routing enabled to distribute load on two application servers in different AZs.
- ☐ D. File a change request to implement Alias Resource Support in the application, use Route 53 Alias Resource Record to distribute load on two application servers in different AZs.

Explanation :

Answer – A

AWS ELB has support for Proxy Protocol. It simply depends on a humanly readable header with the client's connection information to the TCP data sent to your server. As per the AWS documentation, the Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections. Because load balancers intercept traffic between clients and your instances, the access logs from your instance contain the IP address of the load balancer instead of the originating client. You can parse the first line of the request to retrieve your client's IP address and the port number.

- Option A is CORRECT because it implements the proxy protocol and uses ELB with TCP listener.
- Option B is incorrect because, although implementing cross-zone load balancing provides high availability, it is not going to give the IP address of the clients. The answer for B is still wrong because it states to use TCP forwarding, which does not support X-Forwarded-For.
- Option C is incorrect because Route53 latency based routing does not give the IP address of the clients.
- Option D is incorrect because Route53 Alias record does not give the IP address of the clients.

For more information on ELB enabling support for TCP, please refer to the links given below:

- <https://aws.amazon.com/blogs/aws/elastic-load-balancing-adds-support-for-proxy-protocol/> (<https://aws.amazon.com/blogs/aws/elastic-load-balancing-adds-support-for-proxy-protocol/>)
- <https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-proxy-protocol.html> (<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-proxy-protocol.html>)

Ask our Experts



QUESTION 24

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have a periodic Image analysis application that gets some files. The input stream analyzes them and for each file, it writes some data to an output stream to a number of files. The number of files in input per day is high and concentrated in a few hours of the day. Currently, you have a server on EC2 with a large EBS volume that hosts the input data and the results it takes almost 20 hours per day to complete the process

What services could be used to reduce the elaboration time and improve the availability of the solution?

- ☐ A. Use S3 to store I/O files. Use SQS to distribute elaboration commands to a group of hosts working in parallel. Then use Auto scaling to dynamically size the group of hosts depending on the length of the SQS queue. ✓

- ☐ B. Use EBS with Provisioned IOPS (PIOPS) to store I/O files. Use SNS to distribute elaboration commands to a group of hosts working in parallel and Auto Scaling to dynamically size the group of hosts depending on the number of SNS notifications.
- ☐ C. Use S3 to store I/O files, SNS to distribute elaboration commands to a group of hosts working in parallel. Auto scaling to dynamically size the group of hosts depending on the number of SNS notifications.
- ☐ D. Use EBS with Provisioned IOPS (PIOPS) to store I/O files. Use SQS to distribute elaboration commands to a group of hosts working in parallel. Use Auto Scaling to dynamically size the group of hosts depending on the length of the SQS queue.

Explanation :

Answer – A

The scenario in this question is that (a) there are any EC2 instances that need to process high number of input files, (b) currently the processing takes 20 hrs a day, which needs to be reduced, (c) the availability needs to be improved.

Looking at all the options, it appears that there are two choices to be made. (1) between S3 and EBS with PIOPS, and (2) between SQS and SNS.

First, let's see whether we should choose S3 or EBS with PIOPS. It appears that all the options have auto-scaling in common. i.e. there will be multiple EC2 instances working in parallel on the input data. This should reduce the overall elaboration time, satisfying one of the requirements. Since a single EBS volume cannot be attached to multiple instances, using EBS volume seems an illogical choice. Moreover, S3 provides high availability, which satisfies the other requirement.

Second, SQS is a great option to do the autonomous tasks and can queue the service requests and can be scaled to meet the high demand. SNS is a mere notification service and would not hold the tasks. Hence, SQS is certainly the correct choice.

Option A is CORRECT because, as mentioned above, it provides high availability, and can store the massive amount of data. Auto-scaling of EC2 instances reduces the overall processing time and SQS helps distributing the commands/tasks to the group of EC2 instances.

Option B is incorrect because, as mentioned above, neither EBS nor SNS is a valid choice in this scenario.

Option C is incorrect because, as mentioned above, SNS is not a valid choice in this scenario.

Option D is incorrect because, as mentioned above, EBS is not a valid choice in this scenario.

Note:

Option D : It is not correct as single EBS can't be attached to multiple EC2 in auto scaling environment. Only S3 can be correct choice.

Option C: It has S3 but with SNS. As not you know SNS can't be hold task. Hence it is not correct.

Option B: It has both work feature EBS and SNS.

Ask our Experts



QUESTION 25

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You require the ability to analyze a customer's clickstream data on a website so they can do the behavioral analysis. Your customer needs to know what sequence of pages and ads their customer clicked on. This data will be used in real time to modify the page layouts as customers click through the site to increase stickiness and advertising click-through. Which option meets the requirements for captioning and analyzing this data?

- ☐ A. Log clicks in weblogs by URL and store it in Amazon S3, and then analyze with Elastic MapReduce
- ☐ B. Push web clicks by session to Amazon Kinesis and analyze behavior using Kinesis workers ✓
- ☐ C. Write click events directly to Amazon Redshift and then analyze with SQL
- ☐ D. Publish web clicks by session to an Amazon SQS queue and periodically drain these events to Amazon RDS and analyze with sql.

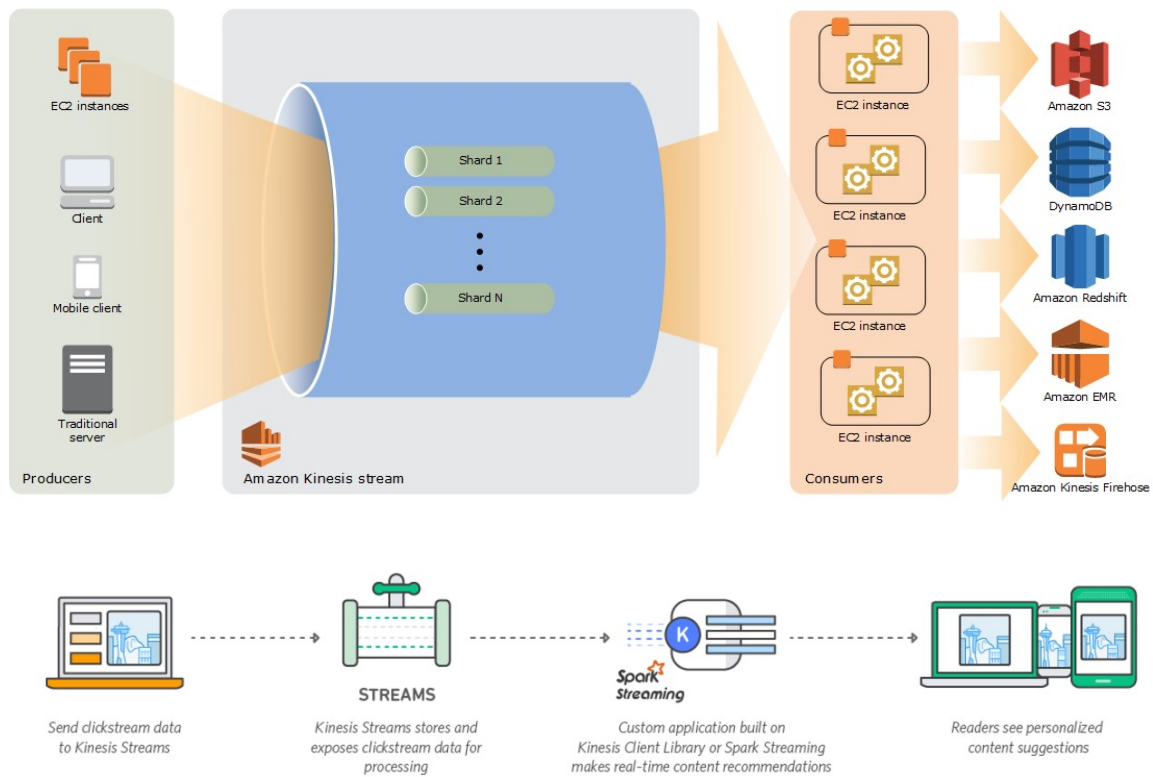
Explanation :

Answer – B

Whenever the question presents a scenario where the application needs to do analysis on real time data such as clickstream (i.e.massive real-time data analysis), most of the time the best option is Amazon Kinesis. It is used to collect and process large streams (<https://aws.amazon.com/streaming-data/>) of data records in real time.

You'll create data-processing applications, known as *Amazon Kinesis Streams applications*. A typical Amazon Kinesis Streams application reads data from an *Amazon Kinesis stream* as data records. These applications can use the Amazon Kinesis Client Library, and they can run on Amazon EC2 instances. The processed records can be sent to dashboards, used to generate alerts, dynamically change pricing and advertising strategies, or send data to a variety of other AWS services

The below diagrams from the aws documentation shows how you can create custom streams in Amazon Kinesis.



For more information on Kinesis, please visit the below link:

<http://docs.aws.amazon.com/streams/latest/dev/introduction.html>
 (http://docs.aws.amazon.com/streams/latest/dev/introduction.html)

Ask our Experts



QUESTION 26

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

An AWS customer runs a public blogging website. The site users upload two million blog entries a month. The average blog entry size is 200 KB. The access rate to blog entries drops to negligible 6 months after publication and users rarely access a blog entry 1 year after publication. Additionally, blog entries have a high update rate during the first 3 months following publication, this drops to no updates after 6 months. The customer wants to use CloudFront to improve his user's load times. Which of the following recommendations would you make to the customer?

- ☐ A. Duplicate entries into two different buckets and create two separate CloudFront distributions where S3 access is restricted only to Cloud Front identity
- ☐ B. Create a CloudFront distribution with "US'Europe price class for US/Europe users and a different CloudFront distribution with All Edge Locations' for the remaining users.
- ☐ C. Create a CloudFront distribution with S3 access restricted only to the CloudFront identity and partition the blog entry's location in S3 according to the month it was uploaded to be used with CloudFront behaviors. ✓
- ☐ D. Create a CloudFront distribution with Restrict Viewer Access Forward Query string set to true and minimum TTL of 0.

Explanation :

Answer – C

The scenario here is that (a) blogs have high access/updates rate in the first 3 months of their creation, (b) this rate drops after 6 months. The main architectural consideration is that the user's load time of the blog needs to be improved.

This question is based on making the best use of CloudFront's Cache Behavior. You need to understand two things about CloudFront for such scenario: (1) CloudFront is a service that is designed to give geographically distributed users the fast access to the content by maintaining the content in the cache that is maintained at multiple edge locations, and (2) using the cache-behavior of CloudFront, you can control the origin and path of the content, time to live (TTL), and control the user access using trusted signers.

In this scenario, you need to control the content based on the time period at which the blog is published. i.e. when a blog is published, you need to cache the update for first 3 months, so that it can be quickly accessed by the users, and after six months from the update, the content can be removed from the cache, as it is rarely accessed. Also, you need to make sure that the content is only accessed by the CloudFront.

Option A is incorrect because maintaining two separate buckets is not going to improve the load time for the users.

Option B is incorrect as the location-wise distribution is not going to improve the load time for the users.

Option C is CORRECT because it (a) the content is only accessed by CloudFront, and (b) if the content is partitioned at the origin based on the month it was uploaded, you can control the cache behavior accordingly, and keep only the latest updated content in the CloudFront cache, so that it can be accessed with fast load-time; hence, improving the performance.

Option D is incorrect. The scenario states that the customer is running a public access blogging website. So there is no need to restrict viewer access.

For more information on Cloudfront identity, please visit the below link

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesCacheBehavior>

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

<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 27

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests, you discover that there is read contention on RDS MySQL. Which are the best approaches to meet these requirements?

Choose 2 options from the below:

- ☐ A. Deploy ElasticCache in-memory cache running in each availability zone ✓
- ☐ B. Implement sharding to distribute load to multiple RDS MySQL instances
- ☐ C. Increase the RDS MySQL Instance size and implement provisioned IOPS
- ☐ D. Add an RDS MySQL read replica in each availability zone ✓

Explanation :

Answer – A and D

The main point to note in this question is that there is a read contention on RDS MySQL. Your should be looking for the options which will improve upon the "read" contention issues. Hint: Always see if any of the options contain (1) caching solution such as ElastiCache, (2) CloudFront, or (3) Read Replicas.

Option A is CORRECT because ElastiCache is a in-memory caching solution which reduces the load on the database and improves the read performance.

Option B is incorrect because sharding does not improve read performance; however, it improves write performance, but write contention is not the issue here.

Option C is incorrect because improving the instance size may improve the read performance, but only up to a specific limit. It is not a reliable solution.

Option D is CORRECT because Read Replicas are used to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Hence, improving the read performance.

See more information on Read Replicas and ElastiCache below.

Read Replicas

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput.

For more information on Read Replica's, please visit the below link:

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

ElastiCache

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

For more information on Amazon ElastiCache, please visit the below link:

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

Ask our Experts



A company is running a batch analysis every hour on their main transactional DB running on an RDS MySQL instance to populate their central Data Warehouse running on Redshift. During the execution of the batch their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data. The dashboard is produced by another system running on-premises that is currently started when a manually-sent email notifies that an update is required. The on-premises system cannot be modified because it is managed by another team.

How would you optimize this scenario to solve performance issues and automate the process as much as possible?

- ☐ A. Replace RDS with Redshift for the batch analysis and SNS to notify the on-premises system to update the dashboard.
- ☐ B. Replace RDS with Redshift for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.
- ☐ C. Create a RDS Read Replica for the batch analysis and SNS to notify the on-premises system to update the dashboard. ✓
- ☐ D. Create a RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.

Explanation :

Answer - C

There are two architectural considerations here. (1) you need to improve read performance by reducing the load on the RDS MySQL instance, and (2) automate the process of notifying to the on-premise system.

When the scenario asks you to improve the read performance of a DB instance, always look for options such as ElastiCache or Read Replicas. And when the question asks you to automate the notification process, always think of using SNS.

Option A is incorrect because Redshift is used for OLAP scenarios whereas RDS is used for OLTP scenarios. Hence, replacing RDS with Redshift is not a solution.

Option B is incorrect because Redshift is used for OLAP scenarios whereas RDS is used for OLTP scenarios. Hence, replacing RDS with Redshift is not a solution.

Option C is CORRECT because (a) it uses Read Replicas which improves the read performance, and (b) it uses SNS which automates the process of notifying the on-premise system to update the dashboard.

Option D is incorrect because SQS is not a service to be used for sending the notification.

For more information on Read Replica's, please visit the below link

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

Ask our Experts



QUESTION 29

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTPS connections to specific domains from their EC2-hosted applications. You deploy a single EC2 instance running proxy software and configure it to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration.

You have a nightly maintenance window of 10 minutes where all instances fetch new software updates. Each update is about 200MB in size and there are 500 instances in the VPC that routinely fetch updates. After a few days you notice that some machines are failing to successfully download some, but not all of their updates within the maintenance window. The download URLs used for these updates are correctly listed in the proxy's whitelist configuration and you are able to access them manually using a web browser on the instances. What might be happening?

Choose 2 answers from the options below:

- ☐ A. You are running the proxy on an undersized EC2 instance type so network throughput is not sufficient for all instances to download their updates in time. ✓
- ☐ B. You have not allocated enough storage to the EC2 instance running the proxy so the network buffer is filling up causing some requests to fail.

- ☐ C. You are running the proxy in a public subnet but have not allocated enough EIP's to support the needed network throughput through the Internet Gateway (IGW).
- ☐ D. You are running the proxy on a appropriate-size EC2 instance in a private subnet and its network throughput is being throttled by a NAT instance running on a t2.micro EC2 instance. ✓
- ☐ E. The route table for the subnets containing the affected EC2 instances is not configured to direct network traffic for the software update locations to the proxy.

Explanation :

Answer : A and D

This scenario contains following main points: (1) there is a single EC2 instance running proxy software that either itself acts as or connects to a NAT instance. The NAT instances are not AWS managed, they are user managed; so, it may become the bottleneck, (2) there is a whitelist maintained so that limited outside access is given to the instances inside VPC, (3) the URLs in the whitelist are correctly maintained, so whitelist is not an issue, (4) only some machines are having download problems with some updates. i.e. some updates are successful on some machines.

This indicates that there is no setup issue, but most-likely it is the proxy instance that is a bottleneck and under-performing or inconsistently performing. As the proxy instance is not part of any auto-scaling group, it's size must be definitely the issue.

Option A is CORRECT because due to limited size of proxy instance, it's network throughput might not be sufficient to provide service to all the VPC instances (as only some of the instances are not able to download the updates).

Option B is incorrect because limited storage on the proxy instance should not cause other instances any problems in downloading the updates.

Option C is incorrect because proxy instances are supposed to be in public subnet, but allocation of EIPs should not cause any issues for other instances in the VPC.

Option D is CORRECT because undersized NAT instance can be a bottleneck and can cause other instances suffer from insufficient network throughput.

Option E is incorrect because if this was the case, none of the instances would get the updates. However, some of the instances were able to get the updates, so, this cannot be the case.

Ask our Experts



To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 large Reserved Instances (RIs) evenly spread across two availability zones. Route 53 is used to deliver the traffic to an Elastic Load Balancer (ELB). After several months, the product grows even more popular and you need additional capacity. As a result, your company purchases two c5.2xlarge RI. You register the two c5.2xlarge instances with your ELB and quickly find that the large instances are at 100% of capacity and the c5.2xlarge instances have a significant capacity that's unused. Which option is the most cost-effective and uses EC2 capacity most effectively?

- ☒ A. Use a separate ELB for each instance type and distribute the load to ELBs with Route53 Weighted Routing.
✓
- ☐ B. Configure AutoScaling group and Launch Configuration with ELB to add up to 10 more on-demand m1 large instances when triggered by Cloudwatch shut off c5.2xlarge instances.
- ☐ C. Route traffic to EC2 large and c5.2xlarge instances directly using Route 53 latency based routing and health checks shut off ELB.
- ☐ D. Configure ELB with two c5.2xlarge Instances and use on-demand AutoScaling group for up to two additional c5.2xlarge instances.

Explanation :

Answer – A

In this question, the problem is that the newly added c5.2xlarge instances are not fully utilized. This is happening because the load is spread evenly across all the instances. There is no logic on how much traffic is to be routed to which instance types.

Hence, there is need to add some logic where higher (more-weighted) traffic should be routed to c5.2xlarge instances and light-weighted to the other instances. Route 53's weighted routing policy does exactly this, so you should look for this option.

Option A is CORRECT because it first creates separate ELBs, one each for set of different instance type and uses Route 53's weighted routing policy such that higher proportion of the load is routed to the ELB that has c5.2xlarge instances and smaller proportion to the one with smaller instances.

Option B is incorrect because shutting down c5.2xlarge instances will not be an effective use of

the EC2 capacity. You have already paid for the instance. So you would lose money here.
Option C is incorrect because latency based routing may not always distribute heavy traffic to the large instance. You must use weighted routing policy.
Option D is incorrect because this option is not a good use of the existing capacity, and in fact, would add to the cost.

For more information on Route 53 weighted routing policy, please visit the URL below:
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-weighted> (<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-weighted>)

Ask our Experts



QUESTION 31

UNATTEMPTED

SCALABILITY & ELASTICITY

A read-only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically. Which AWS services should be used meet these requirements?

- ☐ A. Stateless instances for the web and application tier that are in an auto scaling group, synchronized using Elasticache Memcached and monitored with CloudWatch. RDS configured with read replicas for the backend. ✓
- ☐ B. Stateful instances for the web and application tier in an auto scaling group monitored with CloudWatch, and RDS with read replicas.
- ☐ C. Stateful instances for the web and application tier in an auto scaling group and monitored with CloudWatch, and a multi-AZ RDS.
- ☐ D. Stateless instances for the web and application tier in an auto scaling group that are synchronized using ElastiCache Memcached, and monitored with CloudWatch, and a multi-AZ RDS.

Explanation :

Answer – A

The scenario asks for 2 things: (1) a performance improving solution for read heavy web tier and database tier. Hint: Always see if any of the options contain caching solution such as ElastiCache, CloudFront, or Read Replicas, and (2) whether to use stateless or stateful instances. Stateful instances are not suitable for distributed systems, as they retain the state or connection between client and web server, database remains engaged as long as the session is active. Hence, it increases the load on the server as well as database. Stateless instances, however are distributed and easy to scale in/scale out. Hence, the stateless application tend to improve the performance of a distributed application.

Option A is CORRECT because (a) it uses stateless instances, (b) the web server uses ElastiCache for read operations, (c) it uses CloudWatch which monitors the fluctuations in the traffic and notifies to auto-scaling group to scale in/scale out accordingly, and (d) it uses read replicas for RDS to handle the read heavy workload.

Option B is incorrect because (a) it uses stateful instances, and (b) it does not use any caching mechanism for web and application tier.

Option C is incorrect because (a) it uses stateful instances, (b) it does not use any caching mechanism for web and application tier, and (c) multi-AZ RDS does not improve read performance.

Option D is incorrect because multi-AZ RDS does not improve read performance.

For more information on ElastiCache and Read Replicas, please refer to the following links:

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

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

Ask our Experts



QUESTION 32

UNATTEMPTED

SCALABILITY & ELASTICITY

You are running a news website in the EU-west-1 region that updates every 15 minutes. The website has a worldwide audience. It uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database. Static content resides on Amazon S3 and is distributed through Amazon CloudFront. Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization, you use an Amazon RDS extra large DB instance with 10,000 Provisioned IOPS. Its CPU utilization is around 80%. While freeable memory is in the 2 GB range. Web analytics reports show that the average load time of your web pages is around 1.5

to 2 seconds but your SEO consultant wants to bring down the average load time to under 0.5 seconds. How would you improve page load times for your users? Choose 3 options from the below

- ☐ A. Lower the scale up trigger of your Auto Scaling group to 30% so it scales more aggressively.
- ☐ B. Add an Amazon ElastiCache caching layer to your application for storing sessions and frequent DB queries ✓
- ☐ C. Configure Amazon CloudFront dynamic content support to enable caching of re-usable content from your site ✓
- ☐ D. Switch Amazon RDS database to the high memory extra-large Instance type ✓
- ☐ E. Set up a second installation in another region, and use the Amazon Route 53 latency-based routing feature to select the right region.

Explanation :

Answer – B, C, and D

In this scenario, there are major points of consideration: (1) news website updates every 15 minutes, (2) current average load time is high, and (3) the performance of the use of the website should be improved (i.e. read performance needs improvement). When the questions asks for performance improving solution for read heavy application, always see if any of the options contain caching solution such as ElastiCache, CloudFront, or Read Replicas.

Option A is incorrect because it will increase the number of web server instances, but will not reduce the load on the database; hence, will not improve the read performance.

Option B is CORRECT because it uses ElastiCache for storing sessions as well as frequent DB queries; hence reducing the load on the database. This should help increasing the read performance.

Option C is CORRECT because it uses CloudFront which is a network of globally distributed "edge-locations" that caches the content and improves the user experience.

Option D is CORRECT because scaling up the RDS instance helps improving its read and write performance.

Option E is incorrect because it would not improve read performance; in fact, this setup would add to the cost.

For more information on Elastic Cache, please visit the below URL

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

Dynamic content management via CloudFront can also help alleviate some of the load from the actual web servers.

For more information on Cloudfront Dynamic content, please visit the below URL

<https://aws.amazon.com/cloudfront/dynamic-content/>

(<https://aws.amazon.com/cloudfront/dynamic-content/>)

And finally, since the RDS is at 80% usage, having large instances with better I/O capability can help.

Note:

Amazon CloudFront offers a simple, cost-effective way to improve the performance, reliability and global reach of your entire website for both static content and the dynamic portions of your site that change for each end user. CloudFront's Query string parameters can help you to customize your web pages for each viewer while still taking advantage of the performance and scale benefits offered by caching content at Amazon CloudFront edge locations.

The question says that you have worldwide audience for your website but does not mention whether your audience are equally distributed in all these regions or whether you have more audience in US region and less in Asia-Pacific region etc..

Each of your end users is routed to the Amazon CloudFront edge location closest to them, in terms of internet latency. Then, their requests are carried back to your origin server running in AWS on connections that Amazon monitors and optimizes for performance.

It also reuses existing connections between the Amazon CloudFront edge and the origin server reducing connection setup latency for each origin request.

Considering all these factors, setting up another installation in another region will not provide any better performance and incurs additional cost too. Hence option E may not be a feasible solution in this case.

Ask our Experts



QUESTION 33

UNATTEMPTED

SCALABILITY & ELASTICITY

A large real-estate brokerage is exploring the option of adding a cost-effective location-based alert to their existing mobile application. The application backend infrastructure currently runs on AWS. Users who opt into this service will receive alerts on their mobile device regarding real-estate offers in proximity to their

location. For the alerts to be relevant, delivery time needs to be in the low minute count. The existing mobile app has 5 million users across the US. Which one of the following architectural suggestions would you make to the customer?

- ☐ A. The mobile application will submit its location to a web service endpoint utilizing Elastic Load Balancing and EC2 instances. DynamoDB will be used to store and retrieve relevant offers from EC2 instances which will then communicate with mobile earners/device providers to push alerts back to mobile application.
- ☐ B. Use AWS DirectConnect or VPN to establish connectivity with mobile carriers EC2 instances will receive the mobile applications 'location through carrier connection. RDS will be used to store and relevant offers. EC2 instances will communicate with mobile carriers to push alerts back to the mobile application
- ☐ C. The mobile application will send device location using SQS. EC2 instances will retrieve the relevant offers from DynamoDB. AWS Mobile Push will be used to send offers to the mobile application ✓
- ☐ D. The mobile application will send device location using AWS Mobile Push. EC2 instances will retrieve the relevant offers from DynamoDB. EC2 instances will communicate with mobile carriers/device providers to push alerts back to the mobile application.

Explanation :

Answer – C

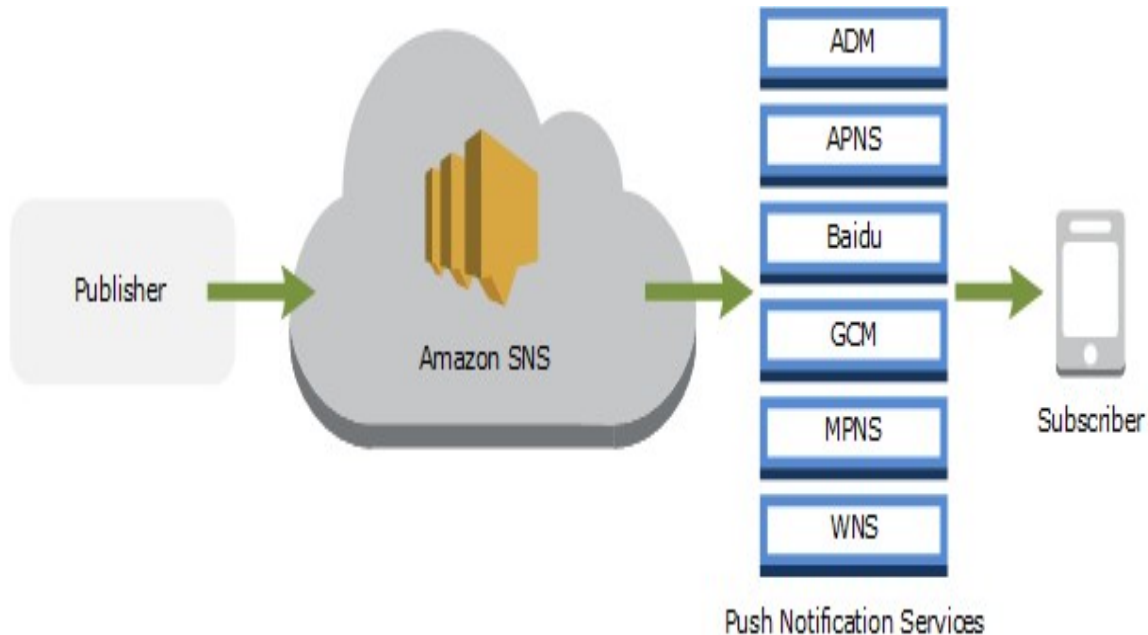
The scenario has following architectural considerations: (1) the users should get notifications about the real estate in the area near to their location, (2) only subscribed users should get the notification, (3) the notification delivery should be fast, (4) the architecture should be scalable, and (5) it should be cost effective.

When the question has considerations for scalability, always think about DynamoDB as it is the most recommended database solution to handle huge amount of data/records. For automated notifications, always think about SNS.

- Option A is incorrect because (a) setting up EC2 instances and ELB to handle 5 millions users will not be cost effective, and (b) sending the notifications via mobile earners/device providers as alerts is neither feasible nor cost effective (certainly not as cost effective as SNS).
- Option B is incorrect because (a) setting up EC2 instances and ELB to handle 5 millions users will not be cost effective, (b) receiving location via Direct Connect and carrier connection is not cost effective, also it does not deal with subscriptions, and (c) sending the notifications via mobile carriers as alerts is not cost effective (certainly not as cost effective as SNS).

- Option C is CORRECT because (a) SQS is a highly scalable, cost effective solution for carrying out utility tasks such as holding the location of millions of users, (b) it uses highly scalable DynamoDB, and (c) it uses the cost effective AWS SNS Mobile Push service to send push notification messages directly to apps on mobile devices.
- Option D is incorrect because AWS SNS Mobile Push service to used for sending push notification messages to the mobile devices, not to get the location of the mobile devices.

For more information on AWS SNS Mobile Push, please see the diagram and link given below:



- <https://docs.aws.amazon.com/sns/latest/dg/SNSMobilePush.html>
(<https://docs.aws.amazon.com/sns/latest/dg/SNSMobilePush.html>)

Note:

The option C says that the mobile application will send device location to the processing EC2 instances using SQS. Then the instances would look at the DynamoDB database for offers relevant to the location. Then finally, AWS Mobile Push, which is part of SNS, will be used to send offers to the mobile application. So it leverages both SQS as well as SNS functionality for different parts of the architecture. This is the correct solution to this problem.

Ask our Experts



A newspaper organization has an on-premises application which allows the public to search its back catalog and retrieve individual newspaper pages via a website written in Java. They have scanned the old newspapers into JPEGs which is of a total size of 17TB and used Optical Character Recognition (OCR) to populate a commercial search product. The hosting platform and software are now end of life. The organization wants to migrate its archive to AWS, produce a cost-efficient architecture, and still be designed for availability and durability. Which of the below options is the most appropriate?

- ☐ A. Use S3 to store and serve the scanned files. Install the commercial search application on EC2 Instances and configure with auto-scaling and an Elastic Load Balancer.
- ☐ B. Model the environment using CloudFormation. Use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index.
- ☐ C. Use S3 to store and serve the scanned files. Use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones. ✓
- ☐ D. Use a single-AZ RDS MySQL instance to store the search index for the JPEG images and use an EC2 instance to serve the website and translate user queries into SQL.
- ☐ E. Use a CloudFront download distribution to serve the JPEGs to the end users and Install the current commercial search product, along with a Java Container for the website on EC2 instances and use Route53 with DNS round-robin.

Explanation :

Answer – C

This question presents following scenarios: (1) type of storage that can store large amount of data (17TB), (2) the commercial search product is at the end of its life, and (3) the architecture should be cost effective, highly available, and durable.

Tip: Whenever a storage service that can store large amount of data with low cost, high availability, and high durability, always think about using S3.

Option A is incorrect because even though it uses S3, it uses the commercial search software which is at the end of its life.

Option B is incorrect because striped EBS is not as durable of a solution as S3 and certainly not as

cost effective as S3. Also, it has maintenance overhead.

Option C is CORRECT because (a) it uses S3 to store the images which is cost-effective, (b) instead of the commercial product that is at its end of life, it uses CloudSearch for query processing, and (c) with multi AZ implementation, it achieves high availability.

Option D is incorrect because with single AZ RDS instance, it does not have high availability.

Option E is incorrect because (a) this configuration is not scalable, and (b) it does not mention any origin for the CloudFront distribution.

Amazon CloudSearch

With Amazon CloudSearch, you can quickly add rich search capabilities to your website or application. You don't need to become a search expert or worry about hardware provisioning, setup, and maintenance. With a few clicks in the AWS Management Console (<https://aws.amazon.com/console/>), you can create a search domain and upload the data that you want to make searchable, and Amazon CloudSearch will automatically provision the required resources and deploy a highly tuned search index.

You can easily change your search parameters, fine tune search relevance, and apply new settings at any time. As your volume of data and traffic fluctuates, Amazon CloudSearch seamlessly scales to meet your needs.

For more information on AWS CloudSearch, please visit the below link:

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

Ask our Experts



QUESTION 35

UNATTEMPTED

COSTING

A company is building a voting system for a popular TV show, viewers watch the performances then visit the show's website to vote for their favorite performer. It is expected that in a short period of time after the show is finished the site will receive millions of visitors. The visitors will be the first login to the site using their Amazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum.

Which of the design patterns below should they use?

- ☐ A. Use CloudFront and an Elastic Load balancer in front of an auto-scaled set of web servers, the web servers will first login with the Amazon service to authenticate the users, then process the users vote and store the result into a multi-AZ Relational Database Service instance.
- ☐ B. Use CloudFront and the static website hosting feature of S3 with the Javascript SDK to call the login with Amazon service to authenticate the user, use IAM Roles to gain permissions to a DynamoDB table to store the users vote.
- ☐ C. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into a DynamoDB table using IAM Roles for EC2 instances to gain permissions to the DynamoDB table.
- ☐ D. Use CloudFront and an Elastic Load Balancer in front of an auto-scaled set of web servers, the web servers will first login with Amazon service to authenticate the user, the web servers will process the users vote and store the result into an SQS queue using IAM Roles for EC2 Instances to gain permissions to the SQS queue. A set of application servers will then retrieve the items from the queue and store the result into a DynamoDB table. ✓

Explanation :

Answer - D

This scenario has following architectural considerations: (1) the application need to be scalable so that it can handle traffic coming from millions of users, (2) the application should handle rapid influx of traffic maintaining good performance, and (3) the cost should be kept to minimum.

When the application needs to handle the data coming from millions of users, always think about using DynamoDB. Also, to provide the global users with high performance content access, you need to consider CloudFront, and you need to set the appropriate IAM Role for the front end / web servers to give access to DynamoDB tables.

- Option A is incorrect because multi-AZ RDS is expensive solution compared to DynamoDB.
- Option B is incorrect because although this would work, it is not scalable and storing all the data directly in DynamoDB would consume read and write capacity and increase the cost.
- Option C is incorrect because it is not scalable and storing all the data directly in DynamoDB would consume read and write capacity and increase the cost.
- Option D is CORRECT because (a) it is highly scalable, (b) creates appropriate IAM Role to access the DynamoDB database, and (c) more importantly uses SQS to hold the user data/votes such that the application does not consume read and write provisioned capacity of DynamoDB.

Note: Option B is scalable but it is only providing us a partial solution.

As per the scenario, once the voting is completed by the user, then the web-page should display the total number of votes submitted online. For that, some processing is required which is not detailed in Option B. But in option D all these steps are provided in the solution.

Option D also includes an Autoscaling group of EC2 instances to handle the traffic.

Hence option D seems to be optimal.

- DynamoDB on-demand is a flexible new capacity mode for DynamoDB capable of serving thousands of requests per second without capacity planning. DynamoDB on-demand offers simple pay-per-request pricing for read and write requests so that you only pay for what you use, making it easy to balance costs and performance.

When you choose on-demand capacity mode, DynamoDB instantly accommodates your workloads as they ramp up or down to any previously reached traffic level. If a workload's traffic level hits a new peak, DynamoDB adapts rapidly to accommodate the workload.

Ask our Experts



QUESTION 36

UNATTEMPTED

COSTING

You are developing a new mobile application and are considering storing user preferences in AWS. This would provide a more uniform cross-device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size. Additionally, 5 million customers are expected to use the application on a regular basis. The solution needs to be cost-effective, highly available, scalable and secure. How would you design a solution to meet the above requirements?

- ☐ **A.** Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials.

- ☐ B. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS, Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access. ✓
- ☐ C. Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data .The mobile application will query the user preferences from the read replicas. Leverage the MySQL user management and access privilege system to manage security and access credentials.
- ☐ D. Store the user preference data in S3. Setup a DynamoDB table with an item for each user and an item attribute pointing to the user' S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly by utilizing STS, Web identity Federation, and S3 ACLs to authenticate and authorize access.

Explanation :

Answer – B

This scenario has following architectural considerations:(1) the application should support millions of customers, so it should be scalable, (2) multiple mobile devices should be able to access the application, and (3) it should be cost effective, highly available and secure.

Tip: Whenever the application needs to (a) support millions of users and scalability is most important, always think about DynamoDB, and (b) give mobile apps the access to AWS resource/service, always think about federated access using Web Identity Provider and "AssumeRoleWithWebIdentity" API.

Option A is incorrect because RDS MySQL is not as scalable and cost-effective as DynamoDB.

Option B is CORRECT because (a) it uses DynamoDB for scalability and cost efficiency, (b) It uses federated access using Web Identity Provider, and (c) uses fine grained access privileges for authenticating the access.

Option C is incorrect because (a) RDS MySQL is not as scalable and cost-effective as DynamoDB, and (b) user management and access privilege system cannot be used for controlling access.

Option D is incorrect because accessing the data via S3 would be slower compared to DynamoDB.

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

<https://aws.amazon.com/dynamodb/developer-resources/>
(<https://aws.amazon.com/dynamodb/developer-resources/>)



QUESTION 37

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Your team has a Tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your organization want access to that same restored data via their EC2 instances in your VPC. What of the following would be the optimal setup for persistence and security that meets the above requirements?

- ☐ A. Create your RDS instance as part of your Elastic Beanstalk definition and alter its security group to allow access to it from hosts in your application subnets.
- ☐ B. Create your RDS instance separately and add its IP address to your application's DB connection strings in your code. Alter its security group to allow access to it from hosts within your VPC's IP address block.
- ☐ C. Create your RDS instance separately and pass its DNS name to your app's DB connection string as an environment variable. Create a security group for client machines and add it as a valid source for DB traffic to the security group of the RDS instance itself. ✓
- ☐ D. Create your RDS instance separately and pass its DNS name to your's DB connection string as an environment variable. Alter its security group to allow access to it from hosts in your application subnets.

Explanation :

Answer - C

The main consideration in this question is: only the EC2 instances in your VPC you should be able to access RDS instances and the setup should support persistence.

Option A is incorrect because RDS instance will be part of the Elastic Beanstalk environment and would not be optimal for persistence.

Option B is incorrect because you should always use the DNS endpoint of the RDS instance, not IP

address as this option suggests.

Option C is CORRECT because (a) it uses RDS instance separately (not part of Beanstalk), (b) it uses DNS name of RDS for accessing it, and (c) it correctly configures the security group such that only the valid client machines have access to RDS instance.

Option D is incorrect because the security group is not configured correctly as it gives access to all the hosts in the application subnets.

Ask our Experts



QUESTION 38

UNATTEMPTED

COSTING

You are looking to migrate your Development and Test environments to AWS. You have decided to use separate AWS accounts to host each environment. You plan to link each accounts bill to a Master AWS account using Consolidated Billing. To make sure you keep within the budget, you would like to implement a way for administrators in the Master account to have access to stop, delete and/or terminate resources in both the Dev and Test accounts. Identify which of the options will allow you to achieve this goal.

- ☐ A. Create IAM users in the Master account with full Admin permissions. Create cross-account roles in the Dev and Test accounts that grant the Master account access to the resources in the account by inheriting permissions from the Master account.
- ☐ B. Create IAM users and a cross-account role in the Master account that grants full Admin permissions to the Dev and Test accounts.
- ☐ C. Create IAM users in the Master account. Create cross-account roles in the Dev and Test accounts that have full Admin permissions and grant the Master account access. ✓
- ☐ D. Link the accounts using Consolidated Billing. This will give IAM users in the Master account access to resources in the Dev and Test accounts

Explanation :

Answer – C

The scenario here is asking you to give permissions to administrators in the Master account such that they can have access to stop, delete, and terminate the resources in two accounts: Dev and Test.

Tip: Remember that you always create roles in the account whose resources are to be accessed. In this example that would be Dev and Test. Then you create the users in the account who will be accessing the resources and give them that particular role. In this example, the Master account should create the users.

Option A is incorrect because the permissions cannot be inherited from one AWS account to another.

Option B is incorrect because cross-account role should be created in Dev and Test accounts, not Master account.

Option C is CORRECT because (a) the cross-account role is created in Dev and Test accounts, and the users are created in the Master account, that are given that role.

Option D is incorrect because consolidated billing does not give access to resources in this fashion.

For more information on cross account access, please visit the below URL

- http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

Ask our Experts



QUESTION 39

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Your customer is willing to consolidate their log streams, access logs, application logs, security logs etc. in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours? What is the best approach to meet your customer's requirements?

- ☐ A. Send all the log events to Amazon SQS. Setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics.

- ☐ B. Send all the log events to Amazon Kinesis. Develop a client process to apply heuristics on the logs ✓
- ☐ C. Configure Amazon Cloud Trail to receive custom logs, use EMR to apply heuristics the logs
- ☐ D. Setup Auto Scaling group of EC2 syslogd servers, store the logs S3 use EMR to apply heuristics on the logs

Explanation :

Answer – B

Whenever the scenario - just like this one - wants to do real-time processing of a stream of data, always think about Amazon Kinesis. Also, remember that the records of the stream is available for 24 hours.

Option A is incorrect because SQS is not used for real time processing of stream of data.

Option B is CORRECT because Amazon Kinesis is best suited for application that does the real-time processing of stream of data. Also, the records of the stream is available for 24 hours in Kinesis.

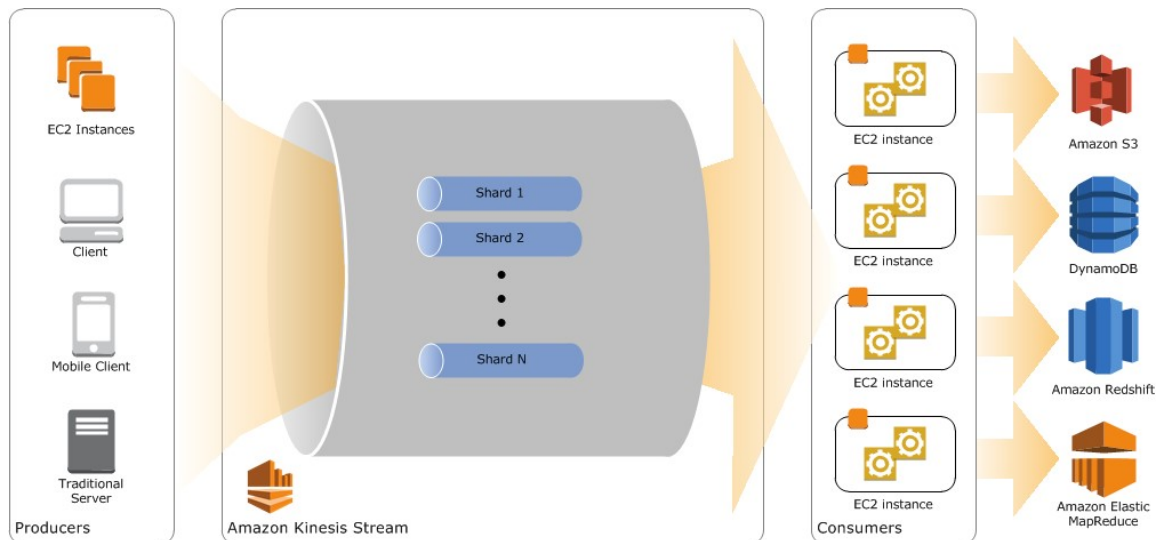
Option C is incorrect because CloudTrail is not used to process the real-time data processing and EMR is used for batch-processing.

Option D is incorrect because setting autoscaling of EC2 instances is not cost-effective and EMR is used for batch-processing.

More information on Amazon Kinesis:

Amazon Kinesis is a platform for streaming data on AWS, making it easy to load and analyze streaming data, and also providing the ability for you to build custom streaming data applications for specialized needs.

- Use Amazon Kinesis Streams to collect and process large streams of data records in real time.
- Use Amazon Kinesis Firehose to deliver real-time streaming data to destinations such as Amazon S3 and Amazon Redshift.
- Use Amazon Kinesis Analytics to process and analyze streaming data with standard SQL.



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

- <https://aws.amazon.com/documentation/kinesis/>
(<https://aws.amazon.com/documentation/kinesis/>)

Ask our Experts



QUESTION 40

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic Map Reduce job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO. You recently improved the overall performance of the website using Cloud Front for dynamic content delivery and your website as the origin. After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude. How will you fix your usage dashboard?

- ☐ A. Enable Cloud Front to deliver access logs to S3 and use them as input of the Elastic Map Reduce job. ✓
- ☐ B. Turn on Cloud Trail and use trail log tiles on S3 as input of the Elastic Map Reduce job
- ☐ C. Change your log collection process to use Cloud Watch ELB metrics as input of the Elastic Map Reduce job

- ☐ D. Use Elastic Beanstalk “Rebuild Environment” option to update log delivery to the Elastic Map Reduce job.
- ☐ E. Use Elastic Beanstalk ‘Restart App server(s)’ option to update log delivery to the Elastic Map Reduce job.

Explanation :

Answer - A

In this scenario, you have a web site that is set up using Elastic Beanstalk. This web site delivers logs to S3, which is used by the EMR job to show the usage dashboard. Now, the architecture is changed, where CloudFront is used to deliver the dynamic content, and is using web site as the origin. The effect that is seen is that the dashboard now shows that the traffic to the website is reduced.

The most likely reason for this is that the dashboard is not getting the true data of the traffic. Since it is unlikely that EMR failed to get the entire data, the most likely cause could be that the S3 may not have the logs of the entire traffic to the website. Hence, most likely reason is that the CloudFront is not sending the logs to S3.

Option A is CORRECT because, as mentioned earlier, if CloudFront delivers the logs to S3, the EMR job will pick those logs and update the dashboard.

Option B is incorrect because the CloudTrail logs would contain the logs about the access of all the AWS resources and APIs, and it will not help updating the dashboard.

Option C is incorrect because CloudWatch metrics logs would not help update the dashboard.

Option D is incorrect because rebuilding environment would not get the logs created by CloudFront in S3. Hence, the dashboard will still not be up-to-date.

Option E is incorrect because restart app servers would not get the logs created by CloudFront in S3. Hence, the dashboard will still not be up-to-date.

More information on CloudFront:

You can configure CloudFront to create log files that contain detailed information about every user request that CloudFront receives. These access logs are available for both web and RTMP distributions. If you enable logging, you can also specify the Amazon S3 bucket that you want CloudFront to save files in.

For more information on Cloudfront logs, please visit the below URL

- <http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>)

Ask our Experts



You are running a successful multitier web application on AWS and your marketing department has asked you to add a reporting tier to the application. The reporting tier will aggregate and publish status reports every 30 minutes from user-generated information that is being stored in your web application's database. You are currently running a Multi-AZ RDS MySQL instance for the database tier. You also have implemented ElastiCache as a database caching layer between the application tier and database tier. Select the answer that will allow you to successfully implement the reporting tier with as little impact as possible to your database.

- ☐ A. Continually send transaction logs from your master database to an S3 bucket and generate the reports off the S3 bucket using S3 byte range requests.
- ☐ B. Generate the reports by querying the synchronously replicated standby RDS MySQL instance maintained through Multi-AZ.
- ☐ C. Launch a RDS Read Replica connected to your Multi AZ master database and generate reports by querying the Read Replica. ✓
- ☐ D. Generate the reports by querying the ElastiCache database caching tier.

Explanation :

Answer – C

In question is asking you to design a reporting layer with least impact on the database. If the reporting queries are fired on the database instance, the performance of the database instance would surely get impacted. Since querying for the report would be a read heavy operation, the best solution is to create the read replicas of the database instance and query on them rather than on the database instance. This way, the existing database instance will have the least impact.

Option A is incorrect because sending the logs to S3 would add to the overhead on the database instance.

Option B is incorrect because you cannot access the standby instance.

Option C is CORRECT because it uses the Read Replicas of the database for the querying of reports.

Option D is incorrect because the querying on ElastiCache may not always give you the latest and entire data, as the cache may not always be up-to-date.

For more information on Read Replica's, please visit the below URL

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

Ask our Experts



QUESTION 42

UNATTEMPTED

SECURITY

A web company is looking to implement an intrusion detection and prevention system for their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC. How should they architect their solution to achieve these goals?

- ☐ A. Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see all traffic across the VPC.
- ☒ B. Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides ✓
- ☐ C. Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
- ☐ D. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Explanation :

Answer - B

This question is asking you to design a scalable IDS/IPS solution (easily applicable to thousands of instances).

There are couple of ways of designing the IDS/IPS systems: (1) install the IDS/IPS agents on each instance in the VPC, and (2) create a separate Security-VPC with only IDS/IPS instances, and route the incoming traffic via this VPC to the other VPC that contains the other EC2 resources.

Option A is incorrect because promiscuous mode is not supported by AWS.

Option B is CORRECT because it creates a second VPC which contains the scalable IDS/IPS

resources, and routes the traffic via these VPC to other VPC.

Option C is incorrect. The incoming traffic should be passed through IDS/IPS before sending it to the servers.

Option D is plausible, but (a) it is not a scalable solution, (b) it is only IDS solution, not IPS solution.

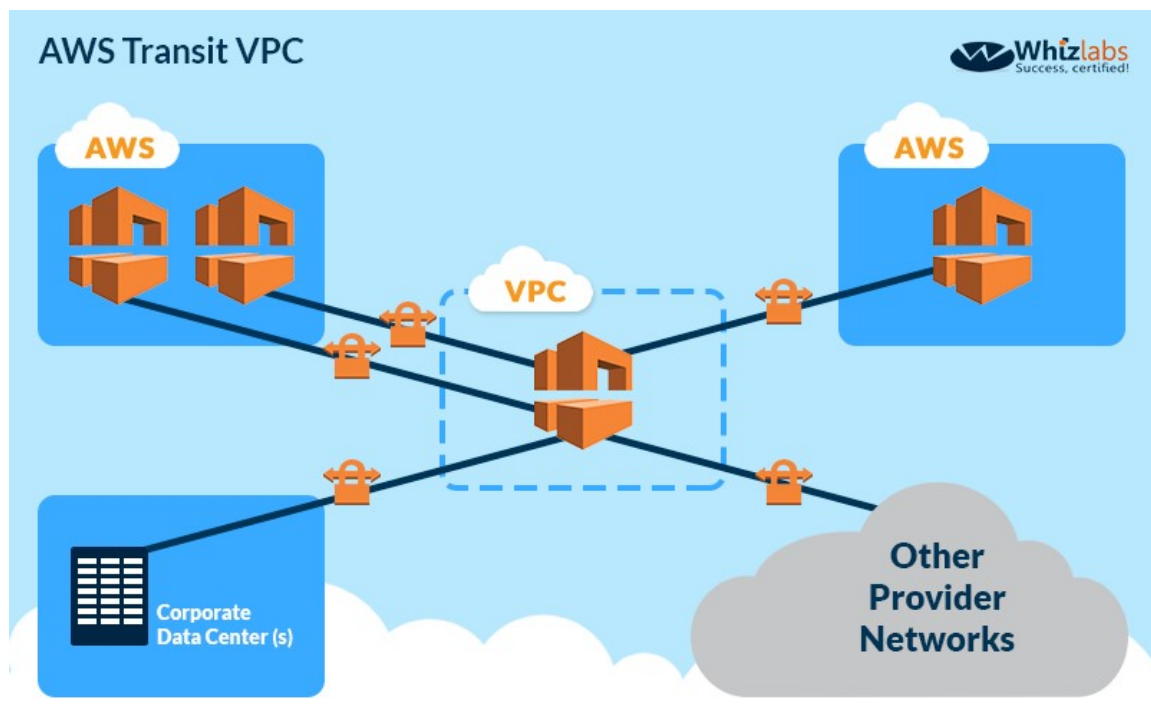
Please visit the URL below for a good slide deck from AWS for getting IDS in place:

<https://awsmedia.s3.amazonaws.com/SEC402.pdf>

(<https://awsmedia.s3.amazonaws.com/SEC402.pdf>)

Note:

You can use this to connect multiple Virtual Private Clouds (VPCs) that might be geographically disparate and/or running in separate AWS accounts, to a common VPC that serves as a global network transit center. This network topology simplifies network management and minimizes the number of connections that you need to set up and manage. Even better, it is implemented virtually and does not require any physical network gear or a physical presence in a colocation transit hub. Here's what this looks like:



- <https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/>
(<https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/>)
- <https://aws.amazon.com/answers/networking/aws-global-transit-network/>
(<https://aws.amazon.com/answers/networking/aws-global-transit-network/>)
- <https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/>
(<https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/>)

- <https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/overview.html>
(<https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/overview.html>)

Ask our Experts



QUESTION 43

UNATTEMPTED

DEPLOYMENT MANAGEMENT

A web-startup runs its very successful social news application on Amazon EC2 with an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application-servers, and DynamoDB as a data store. The main web application best runs on m2 x large instances since it is highly memory- bound. Each new deployment requires the semi-automated creation and testing of a new AMI for the application servers which takes quite a while and is therefore only done once per week. Recently, a new chat feature has been implemented in Node.js and waits to be integrated into the architecture. First tests show that the new component is CPU bound because the company has some experience with using Chef, they decided to streamline the deployment process and use AWS OpsWorks as an application lifecycle tool to simplify management of the application and reduce the deployment cycles. What configuration in AWS OpsWorks is necessary to integrate the new chat module in the most cost-efficient and flexible way?

- ☐ A. Create one AWS OpsWorks stack, create one AWS OpsWorks layer, create one custom recipe.
- ☒ B. Create one AWS OpsWorks stack create two AWS OpsWorks layers, create one custom recipe. ✓
- ☐ C. Create two AWS OpsWorks stacks create two AWS OpsWorks layers, create one custom recipe.
- ☐ D. Create two AWS OpsWorks stacks create two AWS OpsWorks layers, create two custom recipe.

Explanation :

Answer - B

The scenario here requires that you need to manage the application that is created with java, node.js, and DynamoDB using AWS OpsWorks. The deployment process should be streamlined and the deployment cycles should be reduced.

As the java and node.js have different resource requirements, it makes sense to deploy them on different layers. It would make the maintenance easier as well.

Option A is incorrect because it would be a better solution to create two separate layers: one for Java and one for node.js.

Option B is CORRECT because only one stack would be sufficient, and two layers (one for Java and one for node.js) would be required for handling separate requirements. One custom recipe for DynamoDB would be required.

Option C is incorrect because two OpsWork stacks are unnecessary.

Option D is incorrect because two OpsWork stacks are unnecessary.

More information on AWS OpsWork Stack

An AWS OpsWorks Stack defines the configuration of your entire application: the load balancers, server software, database, etc. You control every part of the stack by building layers that define the software packages deployed to your instances and other configuration details such as Elastic IPs and security groups. You can also deploy your software onto layers by identifying the repository and optionally using Chef Recipes to automate everything Chef can do, such as creating directories and users, configuring databases, etc. You can use OpsWorks Stacks' built-in automation to scale your application and automatically recover from instance failures. You can control who can view and manage the resources that are used by your application, including ssh access to the instances that your application uses.

For more information on Ops work, please visit the below URL

<https://aws.amazon.com/opsworks/stacks/faqs/>

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

Ask our Experts



QUESTION 44

UNATTEMPTED

COSTING

Your firm has uploaded a large amount of aerial image data to S3. In the past, in your on-premises environment, you used a dedicated group of servers to process this data and used Rabbit MQ – An open source messaging system to get job information to the servers. Once processed the data would go to the tape and

be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost. Which of the following options is correct?

- ☐ A. Use SQS for passing job messages. Use Cloud Watch alarms to terminate EC2 worker instances when they become idle. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage.
- ☐ B. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Glacier. ✓
- ☐ C. Setup Auto-Scaled workers triggered by queue depth that use spot instances to process messages in SQS. Once data is processed, change the storage class of the S3 objects to Reduced Redundancy Storage (RRS).
- ☐ D. Use SNS to pass the job messages. Use Cloud Watch alarms to terminate spot worker instances when they become idle. Once data is processed, change the storage class of the S3 object to Glacier.

Explanation :

Answer - B

The most suggestive hint in this question is that it asks you to leverage AWS archival storage and messaging services. Hence, you should look for options Glacier and SQS.

Option A is incorrect because (a) RRS is not an archival storage option, and (b) since auto scaling is not mentioned, you cannot use CloudWatch alarms to terminate the idle EC2 instances.

Option B is CORRECT because (a) it uses SQS to process the messages, (b) it uses Glacier as the archival storage solution - which is cost optimized.

Option C is incorrect because RRS is not an archival storage option; instead, use Glacier as it is a low cost archival solution (cost lower than RRS).

Option D is incorrect as SNS cannot be used to process the messages. i.e. it cannot replace the functionality that was getting provided by RabbitMQ.

Ask our Experts



A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an IPsec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user. Which two approaches can satisfy these objectives?

Choose 2 options from the below

- ☐ A. Develop an identity broker that authenticates against IAM Security Token Service (STS) to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.
- ☐ B. The application authenticates against LDAP and retrieves the name of an IAM role associated with the user. The application then calls the IAM Security Token Service (STS) to assume that IAM role. The application can use the temporary credentials to access the appropriate S3 bucket. ✓
- ☐ C. Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service (STS) to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket. ✓
- ☐ D. The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket.

Explanation :

Answer – B and C

There are two architectural considerations here: (1) The users must be authenticated via the on-premise LDAP server, and (2) each user should have access to S3 only.

With this information, it is important to first authenticate the users using LDAP, get the IAM Role name, then get the temporary credentials from STS, and finally access the S3 bucket using those credentials. And second, create an IAM Role that provides access to S3.

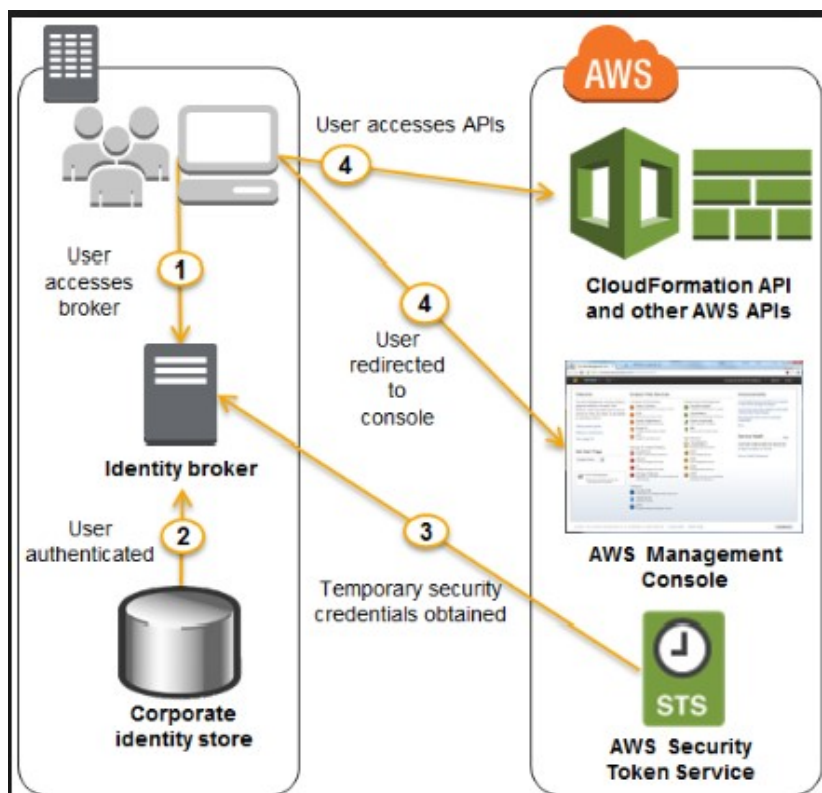
Option A is incorrect because the users need to be authenticated using LDAP first, not STS. Also, the temporary credentials to log into AWS are provided by STS, not identity broker.

Option B is CORRECT because it follows the correct sequence. It authenticates users using LDAP, gets the security token from STS, and then accesses the S3 bucket using the temporary credentials.

Option C is CORRECT because it follows the correct sequence. It develops an identity broker that authenticates users against LDAP, gets the security token from STS, and then accesses the S3 bucket using the IAM federated user credentials.

Option D is incorrect because you cannot use the LDAP credentials to log into IAM.

An example diagram of how this works from the AWS documentation is given below.



For more information on federated access, please visit the below link:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html)



QUESTION 46

UNATTEMPTED

COSTING

Your company is planning to develop an application in which the front end is in .Net and the backend is in DynamoDB. There is expectant of a high load on the application. How could you ensure the scalability and cost-effectiveness of the application to reduce the load on the DynamoDB database? Choose an answer from the below options.

- ☐ A. Add more DynamoDB databases to handle the load.
- ☐ B. Increase write capacity of Dynamo DB to meet the peak loads.
- ☐ C. Use SQS to hold the database requests instead of overloading the DynamoDB database. Then have a service that asynchronously pull the messages and write them to DynamoDB. ✓
- ☐ D. Launch DynamoDB in Multi-AZ configuration with a global index to balance writes.

Explanation :

Answer – C

This question is asking for an option that can be used to reduce the load on DynamoDB database. The option has to be scalable.

In such scenario, the best option to use is SQS, because it is scalable and cost efficient as well.

Option A is incorrect because adding more databases is not going to reduce the load on existing DynamoDB database. Also, this is not a cost efficient solution.

Option B is incorrect because increasing the write capacity is an expensive option.

Option C is CORRECT because it uses SQS to assist in taking over the load from storing the data in DynamoDB, and it is scalable as well as cost efficient.

Option D is incorrect because MultiAZ configuration is not going to help reduce the load, in fact it will affect the performance as the records in DynamoDB would get replicated in multiple availability zones.

More information on SQS:

When the idea comes for scalability then SQS is the best option. Normally DynamoDB is scalable, but since one is looking for a cost effective solution, the messaging in SQS can assist in managing the situation mentioned in the question.

Amazon Simple Queue Service (SQS) is a fully-managed message queuing service for reliably communicating among distributed software components and microservices - at any scale. Building applications from individual components that each perform a discrete function improves scalability and reliability, and is best practice design for modern applications. SQS makes it simple and cost-effective to decouple and coordinate the components of a cloud application. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available

For more information on SQS, please refer to the below URL:
<https://aws.amazon.com/sqs/> (<https://aws.amazon.com/sqs/>)

Ask our Experts



QUESTION 47

UNATTEMPTED

SCALABILITY & ELASTICITY

Your company has 2 departments that want to use Redshift. One department uses a process that takes 3 hours to analyze the data whereas the second department just takes a few minutes. What can you do to ensure that there is no performance impact and delete to the second's department's queries? Choose an answer from the below options.

- ☐ A. Create a read replica of the Red shift instance and run second department's queries on read replica
- ☐ B. Start another Redshift cluster from snapshot for the second department if current Redshift cluster is busy processing long queries
- ☐ C. Pause long queries and resume the queries afterwards
- ☐ D. Create two separate workload management groups and assign them to respective departments ✓

Explanation :

Answer – D

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.

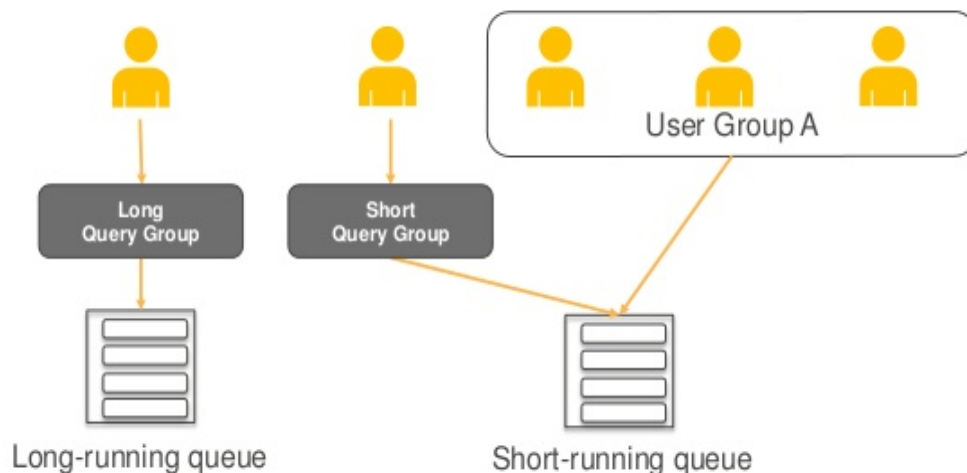
Option B is incorrect because this will affect the performance of the current Redshift cluster.

Option C is incorrect because queries cannot be paused in Redshift.

Option D 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:

Workload Management

Workload management is about creating queues for different workloads



More information on Amazon Redshift Workload Management

Amazon Redshift Workload Management (WLM) enables users to flexibly manage priorities 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 a user 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)



QUESTION 48

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

What can be done in Cloudfront to ensure that as soon as the content is changed in the source, it is delivered to the client? Choose an answer from the options below options.

- ☐ A. Use fast invalidate feature provided in CloudFront.
- ☐ B. Set TTL to 10 seconds.
- ☒ C. Set TTL to 0 seconds. ✓
- ☐ D. Dynamic content cannot be served from the CloudFront.
- ☐ E. You have to contact AWS support center to enable this feature.

Explanation :

Answer - C

In CloudFront, to enforce the delivery of content to the user as soon as it gets changed by the origin, the time to live (TTL) should be set to 0.

Option A is incorrect because invalidate is used to remove the content from CloudFront edge locations cache before it expires. The next time a viewer requests the object, CloudFront fetches the content from the origin; whereas, setting TTL to 0 enforces CloudFront to deliver the latest content as soon as origin updates it.

Option B is incorrect because setting TTL to 10 will keep the content in cache for some time even though origin updates it.

Option C is CORRECT because setting TTL to 0 will enforce the delivery of content to the user as soon as it gets changed by the origin.

Option D is incorrect as CloudFront surely serves dynamic content.

Option E is incorrect as you do not have to contact AWS support center for this scenario.

More information on TTL in CloudFront

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. The low TTL is also given in the AWS documentation.

Low TTLs

Amazon CloudFront uses the expiration period you set on your files (through cache control headers) to determine whether it needs to check the origin for an updated version of the file. If you expect that your files will change frequently, you can set a short expiration period on the file. Amazon CloudFront accepts expiration periods as short as 0 seconds (in which case Amazon CloudFront will revalidate each viewer request with the origin). Amazon CloudFront also honors special cache control directives such as private, no-store, etc.; these are often useful when delivering dynamic content that may not be cached at the edge.

For more information on CloudFront dynamic content, please refer to the below URL:

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

Ask our Experts



QUESTION 49

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

An application has been set up with Autoscaling and EC2 instances in multiple AZ's. When you look at the load balancer logs you notice that EC2 instances in one of the AZ's are not receiving requests. 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

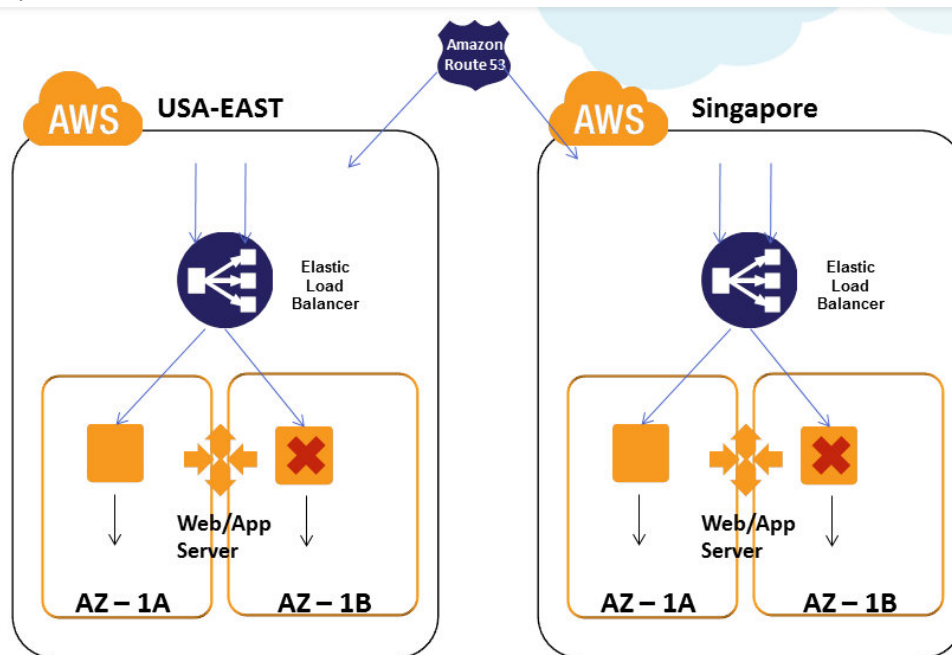
In order to make sure that all the EC2 instances behind a cross-zone ELB receive the requests, make sure that all the applicable availability zones (AZs) are added to that ELB.

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 50

UNATTEMPTED

SECURITY

You want to migrate an EC2 instance from one region to another and use the same PEM keys. How will you accomplish this?

- ☐ A. Key pair is not a region level concept, all the keys are available globally

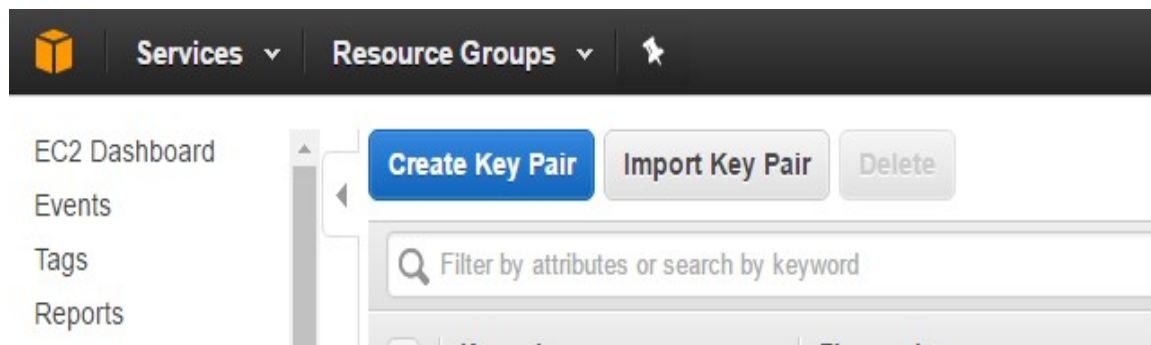
- ☐ B. Use copy key command line API to transfer key to different regions
- ☐ C. Using import key-pair feature using AWS web console ✓
- ☐ D. Copy AMI of your EC2 machine between regions and start an instance from that AMI

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 to 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



Which feature of S3 needs to be enabled for a resource in a bucket in one domain to access a resource in a bucket in another domain? Choose an answer from the below options.

- ☐ A. You can configure your bucket to explicitly enable cross-origin requests from the other domain. ✓
- ☐ B. Modify bucket policy to allow cross domain access.
- ☐ C. Modify the ACL policy to allow cross domain access.
- ☐ D. This is not possible

Explanation :

Answer - A

Option A is CORRECT because CORS enables a resource in one bucket access a resource in another.

Option B is incorrect because you do not need to modify bucket policy.

Option C is incorrect because you do not need to modify ACL policy.

Option D is incorrect as cross bucket access is possible via CORS configuration.

More information on CORS:

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.

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



As a solution architect professional you have been requested to ensure that monitoring can be carried out for EC2 instances which are located in different AWS regions? Which of the below options can be used to accomplish this.

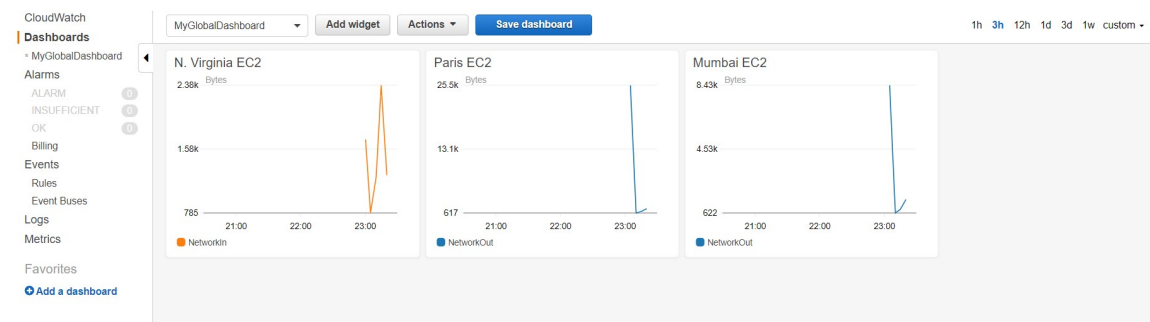
- ☐ A. Create separate dashboards in every region
- ☐ B. Register instances running on different regions to CloudWatch
- ☐ C. Have one single dashboard to report metrics to CloudWatch from different region ✓
- ☐ D. This is not possible

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 snapshot below which shows how a global dashboard looks like:



Option A is incorrect because you can monitor AWS resources in multiple regions using a single CloudWatch dashboard.

Option B is incorrect because you do not need to explicitly register any instances from different regions.

Option C is CORRECT because you can monitor AWS resources in multiple regions using a single CloudWatch dashboard.

Option D is incorrect because as mentioned in option C, the monitoring of EC2 instances is possible using a single dashboard created from CloudWatch matrix.

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 53

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

As an AWS Administrator, you have set up an ELB within a couple of Availability Zones. You have set up a web application on this setup. You notice that the traffic is not being evenly distributed across the AZ's. What can be done to alleviate this issue? Choose an answer from the below options.

- ☐ A. Disable sticky sessions on the ELB. ✓
- ☐ B. Reduce the frequency of the health checks
- ☐ C. Increase the amount of instances hosting the web application in each AZ.
- ☐ D. Recreate the ELB again.

Explanation :

Answer – A

The traffic is not evenly distributed across the instances in multiple AZs. That means the traffic is going to only specific EC2 instances. This happens when either the instances which are not receiving the traffic are unhealthy, or the instances that are receiving the traffic are holding onto the session.

This scenario does not mention about any unhealthy instances. So, it is most likely related to instances holding onto sessions. This means the ELB has sticky sessions enabled.

Option A is CORRECT because this situation occurs when ELB has sticky sessions or session affinity enabled.

Option B is incorrect because reducing the frequency of health checks will not force the even distribution of the traffic.

Option C is incorrect because if sticky sessions are enabled, increasing the number of instances in each AZ will not help receiving the traffic at all. In fact, more instances will remain idle now.

Option D is incorrect because recreating ELB again will not resolve this issue.

More information on ELB Sticky Sessions:

The load balancer uses a special cookie to track the instance for each request to each listener. When the load balancer receives a request, it first checks to see if this cookie is present in the request. If so, the request is sent to the instance specified in the cookie. If there is no cookie, the load balancer chooses an instance based on the existing load balancing algorithm. A cookie is inserted into the response for binding subsequent requests from the same user to that instance. The stickiness policy configuration defines a cookie expiration, which establishes the duration of validity for each cookie.

This could be a reason as to why the sessions are going to a certain AZ.

For more information on ELB sticky sessions, please refer to the below URL

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

Ask our Experts



QUESTION 54

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

As an AWS Cloud Architect professional , 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

It is clearly given in the aws documentation that the Origin Protocol Policy should be set accordingly.

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 on the protocol of the viewer request.

Origin Protocol Policy (Amazon EC2 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 the applicable value:

- **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



QUESTION 55

UNATTEMPTED

NETWORK DESIGN

A company has 2 VPC's in the same region. How can you connect the VPC's so that EC2 instances in one VPC can communicate with the other VPC? Choose an answer from the below options.

- ☐ A. Migrate each VPC resources from one VPC using migration tools such as Import/Export, Snapshot, AMI Copy, and S3 sharing.
- ☐ B. Create a VPC peering connection between each VPC. ✓
- ☐ C. Create a Direct Connect connection from one VPC endpoint to the other VPC.

- ☐ D. Create an OpenVPN instance in one VPC and establish an IPSec tunnel between VPCs.

Explanation :

Answer – B

Option A is incorrect because migration of the resources is unnecessary in this case.

Option B is CORRECT because VPC peering is the best way of connecting the EC2 instances in two VPCs in the same region.

Option C is incorrect because you cannot create Direct Connection between VPCs.

Option D is incorrect because you cannot create IPSec tunnel between VPCs.

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 within a single region.

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>)

Ask our Experts



QUESTION 56

UNATTEMPTED

COSTING

You are designing a multi-platform web application for AWS. The application will run on EC2 instances and will be accessed from PCs, tablets, and smartphones. Supported accessing platforms are Windows, MACOS, IOS, and Android. Separate sticky session and SSL certificate setups are required for different platform types. Which of the following describes the most cost-effective and performance efficient architecture setup?

- ☐ A. Setup a hybrid architecture to handle session state and SSL certificates on-premise and separate EC2 Instance groups running web applications for different platform types running in a VPC.

- ☐ B. Set up an Application Load Balancer with Server Name Indicator support, for handling separate SSL certificate for each device platform. ✓
- ☐ C. Set up two ELBs. The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.
- ☐ D. Assign multiple ELBs to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type. Session stickiness and SSL termination are done at the ELBs.

Explanation :

Answer – B

In this scenario, the main architectural considerations are (1) web application has EC2 instances running multiple platforms such as Android, iOS etc., and (2) separate sticky session and SSL certificate setups are required for different platforms.

The best approach is to create 3 separate ELBs, per platform type.

- Options A is incorrect because it is not cost effective to handle such hybrid architecture.
- Option B is correct. Originally, Application Load Balancers used to support only one certificate for a standard HTTPS listener (port 443) and you had to use Wildcard or Multi-Domain (SAN) certificates to host multiple secure applications behind the same load balancer. The potential security risks with Wildcard certificates and the operational overhead of managing Multi-Domain certificates presented challenges. **With SNI support you can associate multiple certificates with a listener and each secure application behind a load balancer can use its own certificate.** You can use host conditions to define rules that forward requests to different target groups based on the host name in the host header (also known as *host-based routing*). This enables you to support multiple domains using a single load balancer.
- Option C is incorrect because ELB cannot handle multiple SSL certificates.
- Option D is incorrect as it is not required since there is support for multiple TLS/SSL certificates on Application Load Balancers.
- For more information on ELB, please visit the below URL
 - <https://aws.amazon.com/elasticloadbalancing/classicloadbalancer/faqs/>
(<https://aws.amazon.com/elasticloadbalancing/classicloadbalancer/faqs/>)

Ask our Experts



You're consulting for a company that is migrating its legacy application to the AWS cloud. In order to apply high availability, you've decided to implement Elastic Load Balancer and Auto Scaling services to serve traffic to this legacy application.

The legacy application is not a standard HTTP web application but is a custom application with custom codes that is run internally for the employees of the company you are consulting.

The ports required to be open are port 80 and port 8080. Which listener configuration would you create? Choose an answer from the options below:

- ☐ A. Configure the load balancer with the following ports: TCP:80 and TCP:8080 and the instance protocol to TCP:80 and TCP:8080 ✓
- ☐ B. Configure the load balancer with the following ports: HTTP:80 and HTTP:8080 and the instance protocol to HTTPs:80 and HTTPs:8080
- ☐ C. Configure the load balancer with the following ports: HTTP:80 and HTTP:8080 and the instance protocol to TCP:80 and TCP:8080
- ☐ D. Configure the load balancer with the following ports: HTTP:80 and HTTP:8080 and the instance protocol to HTTP:80 and HTTP:8080

Explanation :

Answer – A

The application in this scenario is a legacy based application that is built on TCP and works on ports 80 and 8080. It requires that the traffic should be routed correctly.

Option A is CORRECT, because for the ELB to route the traffic correctly, it should be configured with ports TCP:80 and TCP 8080. For the backends as well, the ports that should be configured must be TCP:80 and TCP:8080.

Option B, C, and D are all incorrect as both the ELB and instance protocol must be configured for ports TCP:80 and TCP:8080.

More information on ELB

Since the application is a custom application and not a standard HTTP application, hence you need to have the TCP ports open. Hence option A is the right option.

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 58

UNATTEMPTED

SECURITY

As an AWS Cloud Architect professional you have been instructed to share files via S3. But since these files are confidential, they cannot be accessed directly and need to be accessed via Cloudfront. Which of the below additional configurations need to be carried out to complete this requirement?

- ☐ 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 the documents are stored in and in that policy grant access to CloudFront only.
- ☐ 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 CloudFront

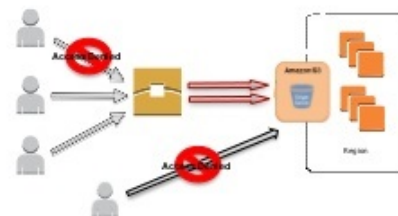
Amazon CloudFront Private Content

(Paid subscribers, premium customers etc.)

Signed URLs or Signed Cookies

When to use?

- Signed URLs: Marketing email
- Signed Cookies: Streaming, whole site authentication



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



You are responsible for a legacy web application whose server environment is approaching end of life. You would like to migrate this application to AWS as quickly as possible, since the application environment currently has the following limitations:

The VM's single 10GB VMDK is almost full. The virtual network interface still uses the 10Mbps driver, which leaves your 100Mbps WAN connection completely underutilized. It is currently running on a highly customized Windows VM within a VMware environment; You do not have the installation media. This is a mission critical application with an RTO (Recovery Time Objective) of 8 hours. RPO (Recovery Point Objective) of 1 hour. How could you best migrate this application to AWS while meeting your business continuity requirements?

- ☒ A. Use the EC2 VM Import Connector for vCenter to import the VM into EC2. ✓
- ☐ B. Use AWS Import/Export to import the VM as an ESS snapshot and attach to EC2.
- ☐ C. Use S3 to create a backup of the VM and restore the data into EC2.
- ☐ D. Use the EC2's bundle-instance API to import an image of the VM into EC2.

Explanation :

Answer – A

Option A is CORRECT because with EC2 VM Import Connector installed, you can import the virtual machines from the VMware vSphere infrastructure into Amazon EC2 using the GUI.

Option B is incorrect because AWS Import/Export is used to transfer large amount of data via to the AWS, not importing the VMs

Option C is incorrect because the backup that is taken and stored on S3 may not be directly restored as an EC2 instance, and (b) it may not meet the RPO of 1 hour as this process will be slow for large number of servers.

Option D is incorrect because (a) it is applicable to only instance store-backed Windows instance and the data on the volumes other than the root device volume does not get preserved, and (b) this API is not applicable to the Windows instances that are backed by EBS volumes.

For more information on EC2 VM Import Connector, please see the URL below:
<https://aws.amazon.com/blogs/aws/ec2-vm-import-connector/>
(<https://aws.amazon.com/blogs/aws/ec2-vm-import-connector/>)

Ask our Experts



QUESTION 60

UNATTEMPTED

NETWORK DESIGN

An administrator in your company has created a VPC with an IPv4 CIDR block 10.0.0.0/24. Now they want to expand the existing VPC size because there is a requirement to host more resources in that VPC. Which of the below requirement can be used to accomplish this? Choose an answer from the below options.

- ☐ A. You cannot change a VPC's size. Currently, to change the size of a VPC you must terminate your existing VPC and create a new one.
- ☒ B. Expand your existing VPC by adding secondary IPv4 IP ranges (CIDRs) to your VPC ✓
- ☐ C. Delete all the subnets in the VPC and expand the VPC.
- ☐ D. Create a new VPC with a greater range and then connect the older VPC to the newer one.

Explanation :

Answer – B

Remember for the exam: In AWS, the CIDR of a VPC **can be** modified after its creation.

Option A is incorrect because you can change the CIDR of VPC by adding upto 4 secondary IPv4 IP CIDRs to your VPC.

Option B is CORRECT because you can expand your existing VPC by adding up to four secondary IPv4 IP ranges (CIDRs) to your VPC.

Option C is incorrect because deleting the subnets is unnecessary.

Option D is incorrect because this configuration would peer the VPC, it will not alter the existing VPC's CIDR.

For more information on VPC and its FAQs, please refer to the following link:

<https://aws.amazon.com/about-aws/whats-new/2017/08/amazon-virtual-private-cloud-vpc-now-allows-customers-to-expand-their-existing-vpcs/> (<https://aws.amazon.com/about-aws/whats-new/2017/08/amazon-virtual-private-cloud-vpc-now-allows-customers-to-expand-their-existing-vpcs/>)

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

Ask our Experts



QUESTION 61

UNATTEMPTED

DEPLOYMENT MANAGEMENT

A company has a legacy based software which needs to be transferred to the AWS cloud. The legacy based software has a dependency on the license which is based on the MAC Address. What would be a possible solution to ensure that the legacy based software will work properly always and not lose the MAC address at any point in time? Choose an answer from the below options.

- ☐ A. Make sure any EC2 Instance that 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 instances having an elastic network interface attached 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 refer to the URL below:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>

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

Ask our Experts



QUESTION 62

UNATTEMPTED

SCALABILITY & ELASTICITY

You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months. Each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS. During the pilot, you measured a peak of 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database. The current deployment consists of a load-balanced auto scaled ingestion layer using EC2 instances and a PostgreSQL RDS database with 500GB standard storage. The pilot is considered a success and your CEO has managed to get the attention from some potential investors. The business plan requires a deployment of at least 100K sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year improvements. To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling.

Which setup will meet the requirements?

- ☐ A. Add an SQS queue to the ingestion layer to buffer writes to the RDS instance.
- ☐ B. Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage.

- ☐ C. Ingest data into a DynamoDB table and move old data to a Redshift cluster. ✓
- ☐ D. Keep the current architecture but upgrade RDS storage to 3TB and 10K provisioned IOPS.

Explanation :

Answer - C

- Option A & D are incorrect because RDS instance will not support the storage of the data for 2 years.
- Option B is incorrect because it does not mention how the ingestion of large data will be handled and how it will get scaled.
- Option C is CORRECT because (a) DynamoDB can handle the large data ingestion, and (b) Redshift can store the data for two years for comparing the improvements.

Note:

During the pilot deployment we have come across an average of 3GB data per month for 100 sensors. We are using a postgres sql of 500GB storage.

The actual requirement is 100,000 sensors which will then produce 3000GB data per month and we need to store it for 24 months which is not practical with the current RDS instance.

Even the 3 TB is also not enough for a period of 24 months.

Ask our Experts



QUESTION 63

UNATTEMPTED

SECURITY

There is a requirement for a web-based application hosted on AWS to talk to Redshift tables. Which of the below options best suited to have this in place from a security standpoint?

- ☐ 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)

Next for any web application, you need to use web identity federation. Hence option D is the right option. This along with the usage of roles is highly stressed in the aws documentation.

" 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)



QUESTION 64

UNATTEMPTED

NETWORK DESIGN

Your company has set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region having distinctive CIDR blocks for each one to connect to the central server having a non conflicting CIDR block. Which of the below options is best suited to achieve this requirement?

- ☐ A. Set up VPC Peering between the central server VPC and each of the teams VPCs. ✓
- ☐ B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.
- ☐ C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
- ☐ D. None of the above options will work.

Explanation :

Answer – A

Option A is CORRECT because VPC Peering allows multiple VPCs to route traffic between them using the private IP addresses of the EC2 instances.

Option B is incorrect because you cannot setup DirectConnect between different VPCs.

Option C is incorrect because you cannot setup IPSec tunnel between different VPCs.

Option D is incorrect as the correct solution is to use VPC Peering.

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

VPC peering needs to have the basic functionality that the CIDR's should not overlap, hence option D is wrong.

For more information on VPC Peering, please visit the link below:
<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>
(<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>)

Ask our Experts



QUESTION 65

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

As an AWS Administrator you are given the following requirement:

- a. MP4 files needing to be streamed publicly on the company's new video website.
- b. The streaming needs to be done on-demand
- c. The video files are archived and are expected to be streamed globally, primarily on mobile devices.

Given the above requirements which of the below options will fulfill the above requirements?

- ☐ 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 configure the Amazon CloudFront Web distribution for streaming the video contents. ✓
- ☐ 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 configure the Amazon CloudFront RTMP distribution for live streaming 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 streaming EC2 instances is a costly solution, (b) the videos are to be delivered on-demand, not live 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 latency when delivering through CloudFront although in most cases, the latency is within acceptable ranges.

For on-demand video streaming, your video content is stored on a server and viewers can watch it at any time

For on-demand video streaming we can deliver the video in two ways. The first method is allowing them to download the entire video and play it and the second option is streaming the video.

For streaming on demand videos, Use the Elastic Transcoder to convert your video files to HLS format (the most widely supported streaming protocol). This will split the video into short segments, and will also create a manifest file. The player uses the manifest file to fetch and play the segments as needed.

- Option D is invalid as it is providing an option for RTMP distribution for live streaming the video contents which is not the requirement.
- <https://aws.amazon.com/blogs/aws/using-amazon-cloudfront-for-video-streaming/>
(<https://aws.amazon.com/blogs/aws/using-amazon-cloudfront-for-video-streaming/>)

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 administer software, scale hardware, tune performance, or otherwise manage transcoding infrastructure. You 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 visit the link below:

- <https://aws.amazon.com/elastictranscoder/> (<https://aws.amazon.com/elastictranscoder/>)

For more information on Using Amazon CloudFront for Video Streaming, please visit the link below:

- <https://aws.amazon.com/blogs/aws/using-amazon-cloudfront-for-video-streaming/>
(<https://aws.amazon.com/blogs/aws/using-amazon-cloudfront-for-video-streaming/>)

Ask our Experts



QUESTION 66

UNATTEMPTED

DEPLOYMENT MANAGEMENT

As an AWS administrator, what is the best way to configure the NAT instance with fault tolerance? Choose the correct answer from the below options.

- ☐ A. Create one NAT instance in a public subnet; create a route from the private subnet to that 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 2 public subnets and 2 private subnets in different AZ where each AZ comprises of one public subnet and one private subnet. Create 2 NAT instance so that each one will reside in a public subnet. Create a route from the private subnet to each NAT instance with in the same AZ, 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.

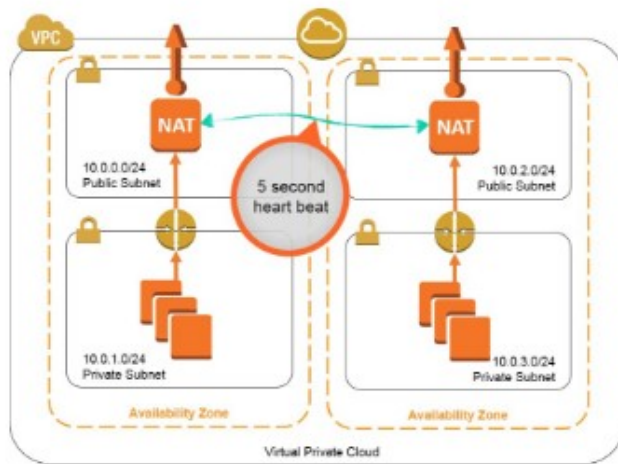
Option C is CORRECT because you should place two NAT instances in two separate public subnets, and create route from instances via each NAT instance for achieving fault tolerance.

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 a 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 67

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

Your company has an on-premises multi-tier PHP web application, which recently experienced downtime due to a large burst in web traffic due to a company announcement. Over the coming days, you are expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructure's ability to handle unexpected increases in traffic.

The application currently consists of a 2 tier web tier which consists of a load balancer and several Linux Apache web servers as well as a database tier which hosts a Linux server hosting a MySQL database.

Which of the below scenarios will provide full site functionality, while helping to improve the ability of your application in the short timeframe required?

- ☐ A. Offload traffic from on-premises environment by setting up a CloudFront distribution and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behaviour, and select a TTL that objects should exist in cache. ✓
- ☐ B. Migrate to AWS. Use VM import 'Export to quickly convert an on-premises web server to an AMI create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic. Create an RDS read replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.
- ☐ C. Create an S3 bucket and configure it for website hosting. Migrate your DNS to Route53 using zone import and leverage Route53 DNS failover to failover to the S3 hosted website.
- ☐ D. Create an AMI which can be used to launch web servers in EC2. Create an Auto Scaling group which uses the AMI's to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance traffic between on-premises web servers and those hosted in AWS.

Explanation :

Answer – A

In this scenario, the major points of consideration are: (1) your application may get unpredictable bursts of traffic, (b) you need to improve the current infrastructure in shortest period possible, and (3) your web servers are on premise.

Since the time period in hand is short, instead of migrating the app to AWS, you need to consider different ways where the performance would improve without doing much modification to the existing infrastructure.

Option A is CORRECT because (a) CloudFront is AWS's highly scalable, highly available content delivery service, where it can perform excellently even in case of sudden unpredictable burst of traffic, (b) the only change you need to make is make the on-premises load balancer as the custom origin of the CloudFront distribution.

Option B is incorrect because you are supposed to improve the current situation in shortest time possible. Migrating to AWS would be more time consuming than simply setting up the CloudFront distribution.

Option C is incorrect because you cannot host dynamic web sites on S3 bucket. Also, this option provides insufficient infrastructure set up options.

Option D is incorrect. It is now possible to use Application Load Balancers through IP Address to On-Premises as well as AWS Resources. However option D is incorrect as it is not covering the database tier which is an essential part of this 2 tier architecture.

More information on CloudFront:

You can have CloudFront sit in front of your on-premise web environment, via a custom origin. This would protect against unexpected bursts in traffic by letting CloudFront handle the traffic from the cache, thus removing some of the load from the on-premise web servers.

Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long-term commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations.

If you have dynamic content, then it is best to have the TTL set to 0.

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

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

Ask our Experts



QUESTION 68

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of spot EC2 instances. Files submitted by your premium customers must be transformed with the highest priority. How should you implement such a system?

- ☐ A. Use a DynamoDB table with an attribute defining the priority level. Transformation instances will scan the table for tasks, sorting the results by priority level.
- ☐ B. Use Route 53 latency based-routing to send high priority tasks to the closest transformation instances.
- ☐ C. Use two SQS queues, one for high priority messages, the other for default priority. Transformation instances first poll the high priority queue; if there is no message, they poll the default priority queue. ✓
- ☐ D. Use a single SQS queue. Each message contains the priority level. Transformation instances poll high-priority messages first.

Explanation :

Answer - C

Option A is incorrect because using DynamoDB tables will be a very expensive solution compared to using SQS queue(s).

Option B is incorrect because the transformation instances are spot instances which may not be up and running all the time; there are chances that they will be terminated.

Option C is CORRECT because (a) it decouples the components of a distributed application, so the application is not impacted due to using spot instances, (b) it is a much cheaper option compared to using DynamoDB tables, and more importantly (b) it maintains a separate queue for the high priority messages which can be processed before the default priority queue.

Option D is incorrect because the transformation instances cannot poll high-priority messages first; they just poll and can determine priority only after receiving the messages.

More information about implementing priority queue via SQS:

<http://awsmedia.s3.amazonaws.com/pdf/queues.pdf>
(<http://awsmedia.s3.amazonaws.com/pdf/queues.pdf>)

Ask our Experts



QUESTION 69

UNATTEMPTED

NETWORK DESIGN

There is a requirement to split a VPC with a CIDR block of 10.0.0.0/24 into two subnets, each of which consists of 128 IP addresses. Can this be done and if so, how will the allocation of IP addresses be configured? Choose the correct answer from the below options.

- ☐ A. One subnet will use CIDR block 10.0.0.0/127 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/255 (for addresses 10.0.0.128 - 10.0.0.255).
- ☐ B. One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.1.0/25 (for addresses 10.0.1.0 - 10.0.1.127).

- ☐ C. One subnet will use CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other will use CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255). ✓
- ☐ D. This is not possible.

Explanation :

Answer – C

This is clearly given in the AWS documentation

" For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255)".

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)

Ask our Experts



QUESTION 70

UNATTEMPTED

NETWORK DESIGN

There is a requirement to change the DHCP options set with a VPC. Which of the following options do you need to take to achieve this?

- ☐ 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

As per the AWS documentation, once you create a set of DHCP options, you cannot modify them.

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.

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 71

UNATTEMPTED

SECURITY

An internal auditor has been assigned to view your company's internal AWS services. As an AWS administrator, what is the best solution to provide the auditor so that he can carry out the required auditing services? Choose the correct answer from the below options.

- ☐ 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.
- ☐ 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/>)

Ask our Experts



QUESTION 72

UNATTEMPTED

NETWORK DESIGN

There is a requirement to host a database server. This server should not be able to connect to the internet except in the case of downloading the required database patches. Which of the following solutions would be the best to satisfy all the above requirements? Choose the correct answer from the below options.

- ☐ 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 database in a private subnet which connects to the Internet via a NAT instance. ✓

Explanation :

Answer – D

Option A 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 outbound traffic via security group as it is stateful.

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 73

UNATTEMPTED

SECURITY

There is a requirement for an application hosted on AWS to work with DynamoDB tables. Which of the following is the best option for the application hosted on an EC2 instance to work with the data in the DynamoDB table? Choose the correct answer from the below options.

- ☐ A. Create an IAM user 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

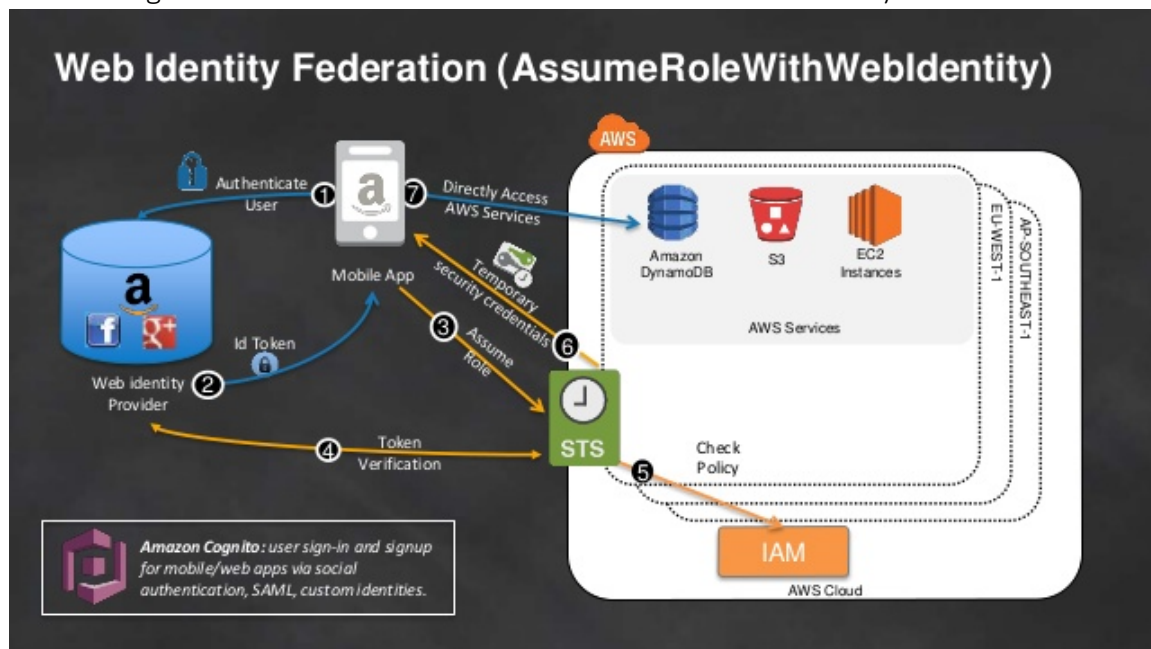
Option A is incorrect because IAM Roles are preferred over IAM Users, because IAM Users have to access the AWS resources using access and secret keys, which is a security concern.

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.



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



As an AWS Administrator, there is a requirement to monitor all changes in an AWS environment and all traffic sent to and from the environment.

Which of the following 2 options can you take into consideration to ensure the requirements are met?

- ☐ 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 promiscuous 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 leaving 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 75

UNATTEMPTED

DEPLOYMENT MANAGEMENT

A legacy application needs to be moved to AWS. But the legacy application has a dependency on multicast? Which of the below options need to be considered to ensure the legacy application works in the AWS environment?

- ☐ 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 76

UNATTEMPTED

SECURITY

An auditor needs read-only access to the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. What is the best way for giving them this sort of access?

- ☐ 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 logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. ✓

Explanation :

Answer – D

Option A is incorrect because just creating a role is not sufficient. CloudTrail logging needs to be enabled as well.

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.

Option D is CORRECT because you need to enable the CloudTrail logging in order to generate the logs with information about all the activities related to the AWS account and resources. It also creates an IAM user that has permissions to read the logs that are stored in the S3 bucket.

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 77

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

There is a requirement to have the read replica of a running MySQL RDS instance inside of AWS to an on-premise location. What is the securest way of performing this replication? Choose the correct answer from the below options.

- ☐ 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. Create an IPSec VPN connection using either OpenVPN or VPN/VGW through the Virtual Private Cloud service. ✓

Explanation :

Answer – D

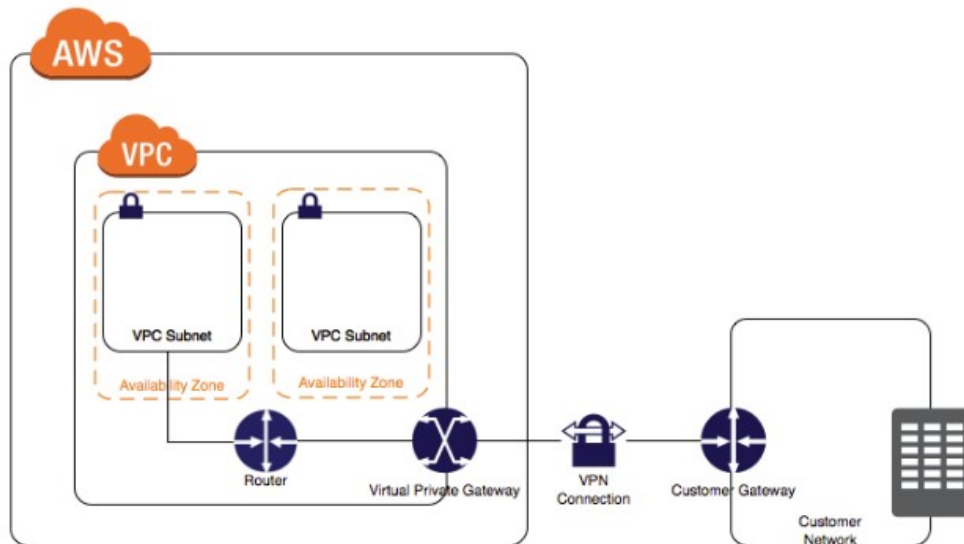
Option A is incorrect because SSL endpoint cannot be used here as it is used for securely accessing the database.

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)

Ask our Experts



QUESTION 78

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

Your company produces customer commissioned one-of-a-kind skiing helmets combining high fashion with custom technical enhancements. The current manufacturing process is data rich and complex including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards. Assessments are a mixture of human and automated assessments you need to add a new set of assessment to model the failure modes of the custom electronics using GPUs across a cluster of servers with low latency networking. What architecture would allow you to automate the existing process using a hybrid approach and ensure that the architecture can support the evolution of processes over time?

- ☐ A. Use AWS Data Pipeline to manage movement of data & meta-data and assessments. Use an auto-scaling group of G3 instances in a placement group.

- ☐ B. Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an autoscaling group of G3 instances in a placement group. ✓
- ☐ C. Use Amazon Simple Workflow (SWF) to manage assessments movement of data & meta-data. Use an autoscaling group of C3 instances with SR-IOV (Single Root I/O Virtualization).
- ☐ D. Use AWS data Pipeline to manage movement of data & meta-data and assessments. Use auto-scaling group of C3 with SR-IOV (Single Root I/O virtualization).

Explanation :

Answer - B

Tip: Whenever the scenario in the question mentions about high graphical processing servers with low latency networking, always think about using G3 instances. And, when there are tasks involving human intervention, always think about using SWF.

Option A is incorrect because AWS Data Pipeline cannot work in hybrid approach where some of the tasks involve human actions.

Option B is CORRECT because (a) it uses G3 instances which are specialized for high graphical processing of data with low latency networking, and (b) SWF supports workflows involving human interactions along with AWS services.

Option C is incorrect because it uses C3 instances which are used for situations where compute optimization is required. In this scenario, you should be using G3 instances.

Option D is incorrect because (a) AWS Data Pipeline cannot work in hybrid approach where some of the tasks involve human actions, and (b) it uses C3 instances which are used for situations where compute optimization is required. In this scenario, you should be using G3 instances.

More information on G3 instances:

Using G3 instances is preferred. Hence option C and D are wrong.

P3
P2
G3
F1

G3 instances are optimized for graphics-intensive applications.

Features:

- High frequency Intel Xeon E5-2686 v4 (Broadwell) processors
- NVIDIA Tesla M60 GPUs, each with 2048 parallel processing cores and 8 GiB of video memory
- Enables NVIDIA GRID Virtual Workstation features, including support for 4 monitors with resolutions up to 4096x2160. Each GPU included in your instance is licensed for one "Concurrent Connected User"
- Enables NVIDIA GRID Virtual Application capabilities for application virtualization software like Citrix XenApp Essentials and VMware Horizon, supporting up to 25 concurrent users per GPU
- Each GPU features an on-board hardware video encoder designed to support up to 10 H.265 (HEVC) 1080p30 streams and up to 18 H.264 1080p30 streams, enabling low-latency frame capture and encoding, and high-quality interactive streaming experiences
- Enhanced Networking using the Elastic Network Adapter (ENA) with 25 Gbps of aggregate network bandwidth within a Placement Group

Model	GPUs	vCPU	Mem (GiB)	GPU Memory (GiB)	Network Performance
g3s.xlarge	1	4	30.5	8	Up to 10 Gigabit
g3.4.xlarge	1	16	122	8	Up to 10 Gigabit
g3.8.xlarge	2	32	244	16	10 Gigabit
g3.16.xlarge	4	64	488	32	25 Gigabit

All instances have the following specs:

- 2.3 GHz (base) and 2.7 GHz (turbo) Intel Xeon E5-2686 v4 Processor
- Intel AVX, Intel AVX2, Intel Turbo
- EBS Optimized
- Enhanced Networking†

Use Cases

3D visualizations, graphics-intensive remote workstation, 3D rendering, application streaming, video encoding, and other server-side graphics workloads.

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

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

Since there is an element of human intervention, SWF can be used for this purpose.

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

- <https://aws.amazon.com/swf/> (<https://aws.amazon.com/swf/>)

Ask our Experts



There is a requirement for a company to transfer large amounts of data between AWS and an on-premise location. There is an additional requirement for low latency and high consistency traffic to AWS. Out of these given requirements, how would you design a hybrid architecture? Choose the correct answer from the below options.

- ☐ A. Provision a Direct Connect connection to an AWS region using a Direct Connect partner. ✓
- ☐ B. Create a VPN tunnel for private connectivity which increases network consistency and reduces latency.
- ☐ C. Create an IPSec tunnel for private connectivity which increases network consistency and reduces latency.
- ☐ D. This is not possible.

Explanation :

Answer – A

Tip: Whenever the scenario in the question requires the use of low latency transfer of data between AWS/VPC and on-premise servers/database, always think about provisioning AWS Direct Connect.

Option A is CORRECT because Direct Connect creates a dedicated connection between AWS and on-premise server for low latency secured transfer of data.

Option B is incorrect because setting up VPN connectivity has higher cost as well as setup and maintenance overhead compared to Direct Connect. Also, Direct Connect provides a dedicated network connection bypassing the internet. Hence it is more secure.

Option C is incorrect because setting up IPSec tunnel has setup and maintenance overhead. Also, IPSec tunnel does not guarantee the end-to-end security of the data as it uses internet.

Option D is incorrect as Direct Connect is the most suited option for this scenario.

More information on AWS Direct Connect:

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

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 80

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

You're running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible block-based storage. You have 624TB of data and would like to mount it as a single folder on your file server. Users must be able to access portions of this data while the backups are taking place. What backup solution would be most appropriate for this use case?

- ☐ A. Use Storage Gateway and configure it to use Gateway Cached volumes. ✓
- ☐ B. Configure your backup software to use S3 as the target for your data backups.
- ☐ C. Configure your backup software to use Glacier as the target for your data backups.
- ☐ D. Use Storage Gateway and configure it to use Gateway Stored volumes.

Explanation :

Answer - A

Gateway-Cached volumes can support volumes of 1,024TB in size, whereas Gateway-stored volume supports volumes of 512 TB size.

Option A is CORRECT because (a) it supports volumes of up to 1,024TB in size, and (b) the frequently accessed data is stored on the on-premise server while the entire data is backed up over AWS.

Option B is incorrect because S3 is not ideal for POSIX compliant data.

Option C is incorrect because the data stored in Amazon Glacier is not available immediately. Retrieval jobs typically require 3–5 hours to complete; so, if you need immediate access to your data as mentioned in the question, this may not be the ideal choice.

Option D is incorrect because gateway stored volumes can only store only 512TB worth of data.

For more information on all of the options for storage please refer to the below link

<http://docs.aws.amazon.com/storagegateway/latest/userguide/resource-gateway-limits.html#resource-volume-limits>
(<http://docs.aws.amazon.com/storagegateway/latest/userguide/resource-gateway-limits.html#resource-volume-limits>)

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13604>)

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/>)

Mobile App

 Android Coming Soon

 iOS Coming Soon

Company

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

Follow us



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



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



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



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

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