

[🏠 \(https://www.whizlabs.com/learn/\)](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 II \(https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13605\)](https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13605) > **Report**

PRACTICE TEST II

Attempt 1

Marks Obtained 1 / 80

Your score is 1.25%

Completed on Tuesday , 29 January 2019 , 01:37 PM

Time Taken 00 H 00 M 38 S

Result Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	High Availability and Business Continuity	17	1	0	16
2	Costing	8	0	0	8
3	Security	18	0	0	18
4	Network Design	7	0	0	7
5	Cloud Migration & Hybrid Architecture	8	0	0	8
6	Deployment Management	13	0	0	13
7	Data Storage	4	0	0	4
8	Scalability & Elasticity	5	0	0	5

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

Show Answers

All



QUESTION 1

CORRECT

HIGH AVAILABILITY AND BUSINESS CONTINUITY

As an AWS professional, you have been told to ensure that traffic to an application is evenly balanced. The application has multiple web servers that host the application. Choose an answer from the below options which will fulfill the above requirement.

- ☐ A. Configure a NAT instance in your VPC 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 ALIAS record to your CloudFront distribution.
- ☒ C. Place all your web servers behind ELB. Configure a Route53 ALIAS to point to the ELB DNS name. ✓
- ☐ D. Configure ELB with an EIP. Place all your Web servers behind ELB Configure a Route53 A record that points to the EIP.

Explanation :

Answer – C

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 'ALIAS' 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. The question does not mention the presence of an ELB.

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: d111111abcdef8.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 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://aws.amazon.com/elasticloadbalancing/>)

Ask our Experts



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 that you may need to pay for a consultant.

How do 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/>)

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

Ask our Experts



QUESTION 3

UNATTEMPTED

COSTING

Your company is hosting an application on the cloud. Your IT Security department has recently noticed that there seem to be some SQL Injection attacks against the application. Which of the below approach provides a cost-effective scalable mitigation to this kind of attack?

- ☐ A. Create a DirectConnect connection so that you have a dedicated connection line.
- ☐ B. Add previously identified host file source IPs as an explicit INBOUND DENY NACL to the web tier subnet.

- ☐ C. Use WAF to protect applications that are running behind an Application Load Balancer. ✓
- ☐ 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, always think of using Web Access Firewall (WAF).

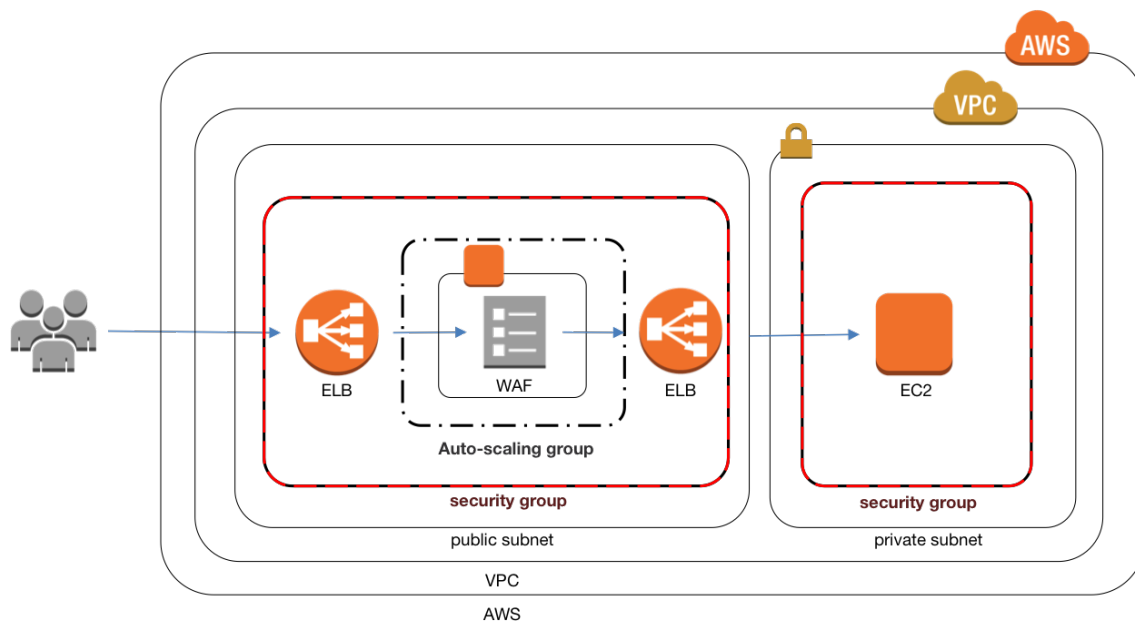
AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining 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 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 4

UNATTEMPTED

SECURITY

Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your AWS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you recommend?

- ☐ A. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM roles S3 bucket policies and Multi Factor Authentication (MFA) 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 global services option selected. Use S3 ACLs and Multi Factor Authentication (MFA) 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 :

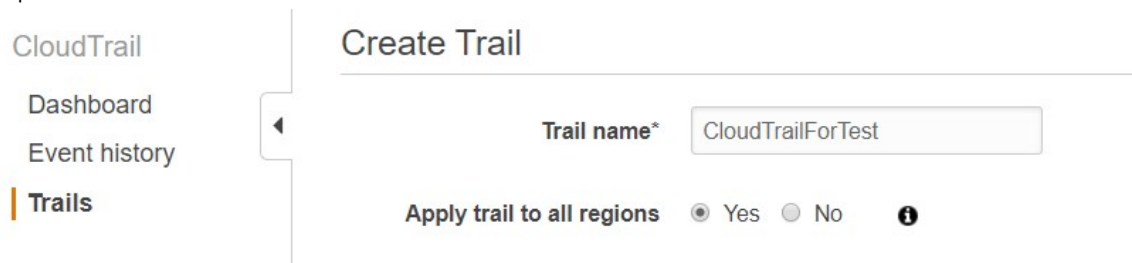
Answer – A

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) S3 bucket with global services option enabled, (b) Data integrity, and (c) Confidentiality.

Option A is CORRECT because (a) it uses AWS CloudTrail with Global Option 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 Global Option.



Options B is incorrect because (a) although it uses AWS CloudTrail, the Global Option 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 Global Option 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 5

UNATTEMPTED

SECURITY

A company has recently started using Docker cloud. This is a SaaS solution for managing Docker containers on the cloud. There is a requirement for the SaaS solution to access AWS resources. Which of the following options would meet the requirement in the most secured way assuming that the SaaS provider is also on AWS platform?

- ☐ 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 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 that allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider to use 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 it's 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 have instances in a public subnet which downloads patches from the internet in addition to serving clients on the normal HTTP protocol. There is a requirement to ensure that just the serving protocol and the URL's listed to get the patches are accessible from the instances. Which of the following options would you consider?

- ☐ A. Configure a web proxy server in your VPC and enforce URL-based rules for outbound access. Remove default routes. ✓
- ☐ B. Implement security groups and configure outbound rules to only permit traffic to the url's.
- ☐ 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 all specific destinations, with an Implicit deny as a rule.

Explanation :

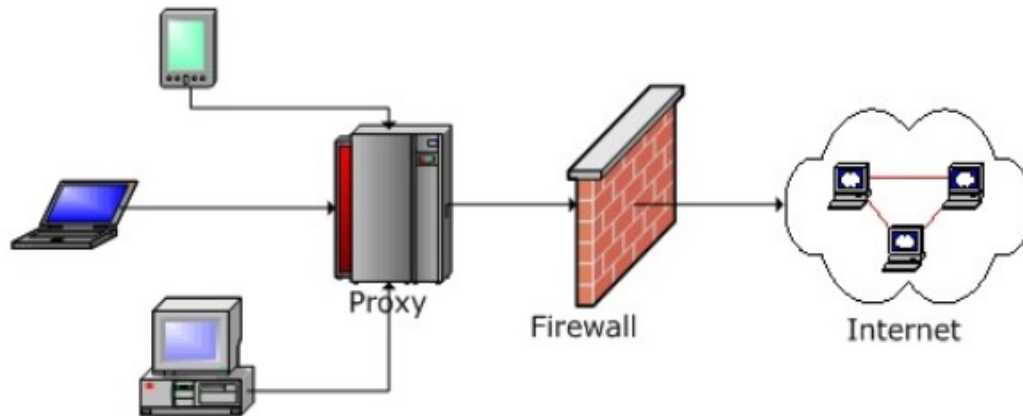
Answer – A

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.

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.

Option D is incorrect because a Network Access Control lists cannot filter request based on URLs.

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>)

Note:

As per AWS,

You cannot delete the main route table, but you can replace the main route table with a custom table that you've created (so that this table is the default table each new subnet is associated with).

The main route table controls the routing for all subnets that are not explicitly associated with any other route table. You can add, remove, and modify routes in the main route table.

So in this case we are not deleting the default main route table but we are removing the default routes from it.

Ask our Experts



Your company has recently extended its datacenter into a VPC on AWS. There is a requirement for on-premise users to manage AWS resources from the AWS console. You don't want to create IAM users for them again. Which of the below options will fit your needs for authentication?

- ☐ 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:

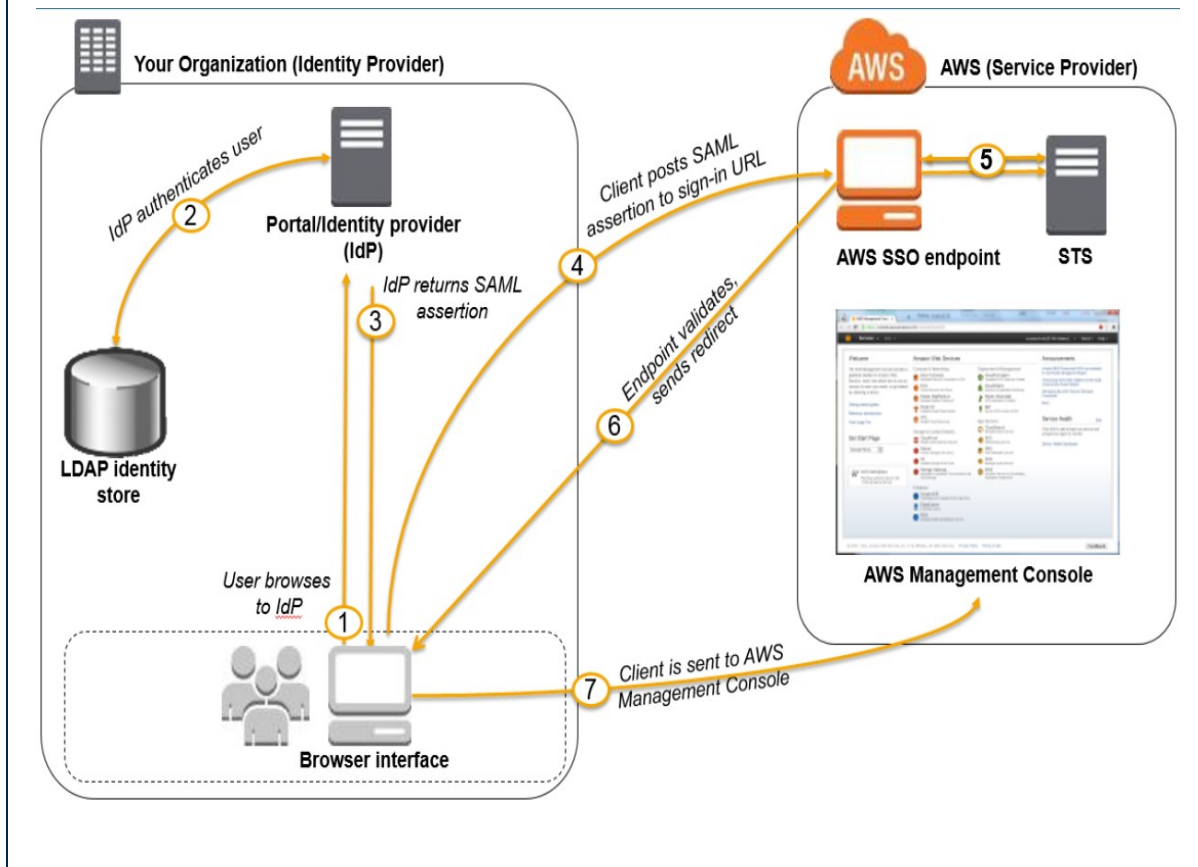
- <https://aws.amazon.com/identity/federation/>
(<https://aws.amazon.com/identity/federation/>)

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 we are not using Web Identity Federation as it is used with public identity providers such as Facebook, Google etc.
- 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



What are the benefits of using an IPSec tunnel from connecting from an on-premise location to AWS?

Choose 4 correct options from the below:

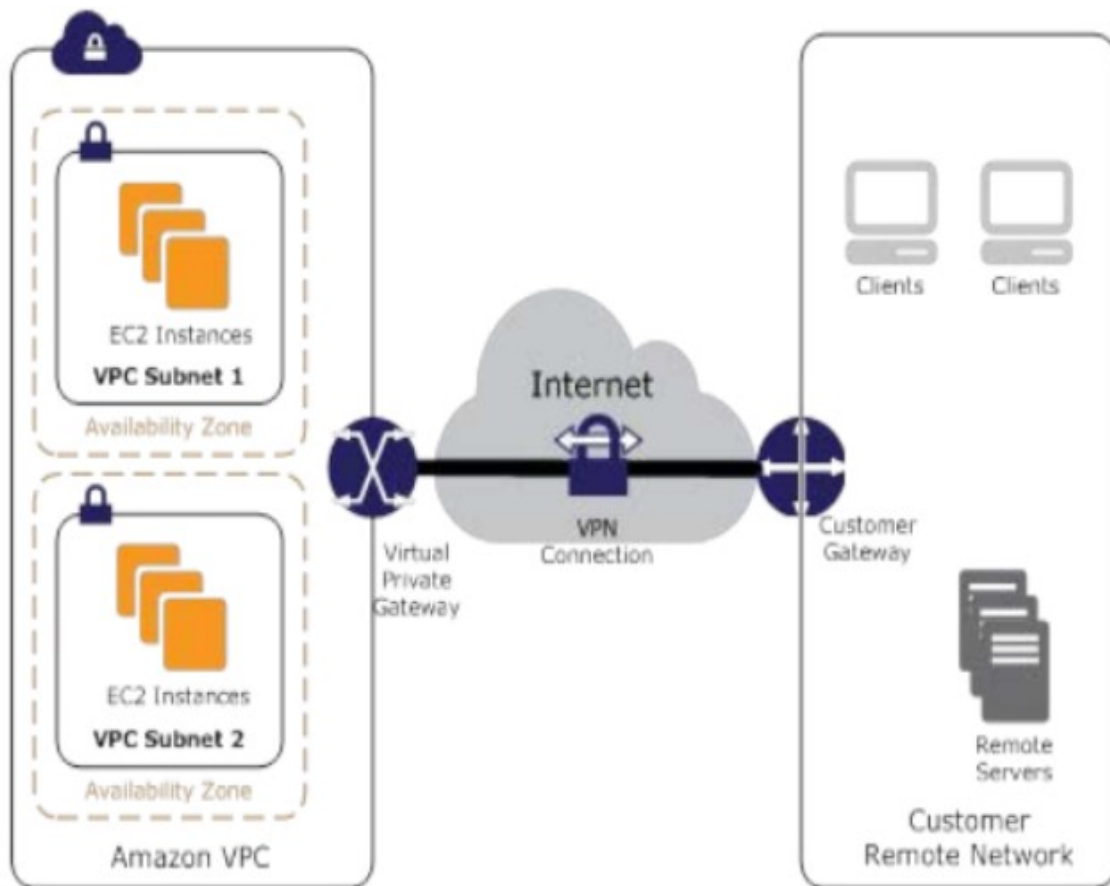
- ☐ A. End-to-end protection of data in transit
- ☐ B. End-to-end Identity authentication
- ☐ C. Data encryption across the Internet ✓
- ☐ D. Protection of data in transit over the Internet ✓
- ☐ E. Peer identity authentication between VPN gateway and customer gateway ✓
- ☐ F. Data integrity protection 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, the IPSec tunnel is established between VPN gateway (VPG) and Customer Gateway (CGW) whose identity gets authenticated during the setup of the IPSec tunnel.

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 9

UNATTEMPTED

NETWORK DESIGN

What should you consider when you try to implement an IDS infrastructure on AWS?

Choose 2 correct 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 10

UNATTEMPTED

SECURITY

An application store a set of files in a single Amazon S3 bucket. Users will upload files from their mobile device directly to Amazon S3 and will be able to view and download their uploaded files directly from Amazon S3. You want to configure security to handle potentially millions of users in the most secure manner possible. What should your server-side application do when a new user registers on the 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 funtions such as "AssumeRole", "AssumeRoleWithSAML", and "AssumeRoleWithWebIdentity". See the following diagram that explains the flow of actions while using "AssumeRole".

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)

Note:

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.

Ask our Experts



QUESTION 11

UNATTEMPTED

SECURITY

You have an application running on an EC2 Instance access an S3 bucket. 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



Which of the following are the recommendations from AWS when migrating a legacy application which is hosted on a virtual machine in an on-premise location?

Choose 2 options from the below:

- ☐ A. Use a NAT instance to route traffic from the instance in the VPC.
- ☐ B. Use an Elastic IP address on the VPC instance ✓
- ☐ C. Use entries in Amazon Route 53 that allow the Instance to resolve its dependencies' IP addresses on the on-premise location
- ☐ D. Use the VM Import facility provided by aws. ✓

Explanation :

Answers: B and D

Option A is incorrect because having NAT instance is not going to help in this scenario. NAT instance is used so that the instances in the private subnet can communicate with the internet.

Option B is CORRECT because using an elastic IP address you can mask the failure of an instance or the legacy app in this case by remapping the IP address to another functioning instance in a VPC subnet.

Option C is incorrect because Route 53 cannot resolve any dependencies on the IP addresses.

Option D is CORRECT because VM Import/Export enables you to easily import VM images from the on-premise location to the VPC in the form of EC2 instances, hence helping the migration of the legacy application.

Ask our Experts



You are designing an application 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 tiers; also use Amazon Relational Database Service (RDS) ✓
- ☐ 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 14

UNATTEMPTED

SECURITY

A company has a web application hosted on AWS. The IT Security Administrator has noticed that a lot of requests are coming from a set of IPs. As an AWS professional, what can you do to ensure that this type of attack is limited?

- ☐ A. Create a custom route table associated with the web tier and block the attacking IP addresses from the IGW (internet Gateway)
- ☐ B. Create web Security Group rules to block the attacking IP addresses over port 80
- ☐ C. Put the application on the private subnet.

- ☐ 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 (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 C is incorrect because if the application servers are put in the private subnet, the application will not be accessible from the internet, especially since the option does not mention any public facing ELB or Route 53 configuration.

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

Ask our Experts



Which of the following options 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.

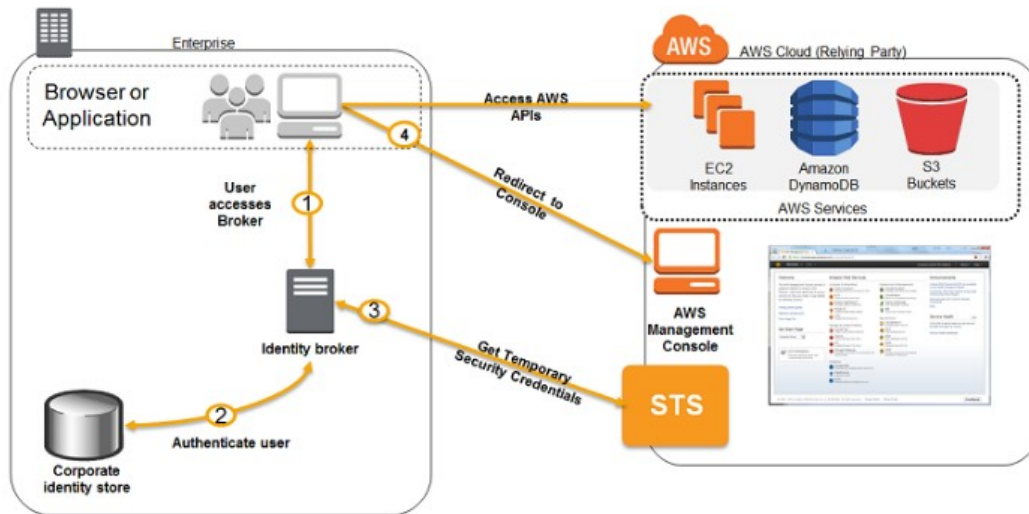
Option B is CORRECT because as mentioned above, getting temporary access tokens / credentials using AWS STS is needed.

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 (a) 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 16

UNATTEMPTED

SECURITY

When one creates an encrypted EBS volume and attach it to a supported instance type, which of the following data types are encrypted?

Choose 3 options from the below:

- ☐ A. Data at rest inside the volume ✓
- ☐ B. All data copied from the EBS volume to S3
- ☐ C. All data moving between the volume and the instance ✓
- ☐ D. All snapshots created from the volume ✓

Explanation :

Answer – A, C, and D

Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

- (i) Data at rest inside the volume
- (ii) All data moving between the volume and the instance
- (iii) All snapshots created from the volume
- (iv) All volumes created from those snapshots

Based on this, options A, B, and D are all CORRECT.

Option B is incorrect since the data that is copied to S3 is not encrypted.

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

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

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

Ask our Experts



QUESTION 17

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

- ☐ B. EBS with Provisioned IOPS (PIOPS) 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
- ☐ C. S3 to store I/O files, SNS to distribute evaporation 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. EBS with Provisioned IOPS (PIOPS) to store I/O files 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.

Ask our Experts



QUESTION 18

UNATTEMPTED

DEPLOYMENT MANAGEMENT

A company has the requirement to analyze the clickstreams from a web application. Which of the below options will fulfill this requirement?

- ☐ 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. Then, analyze with SQL

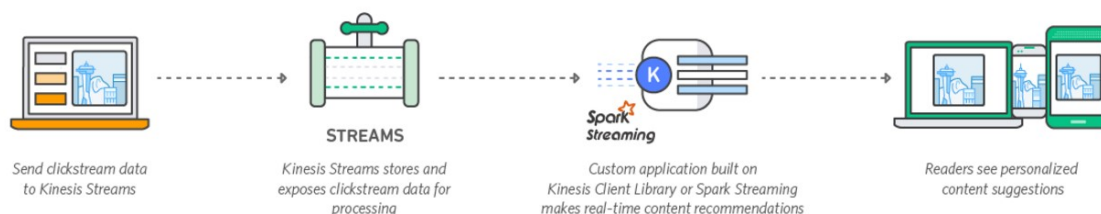
Explanation :

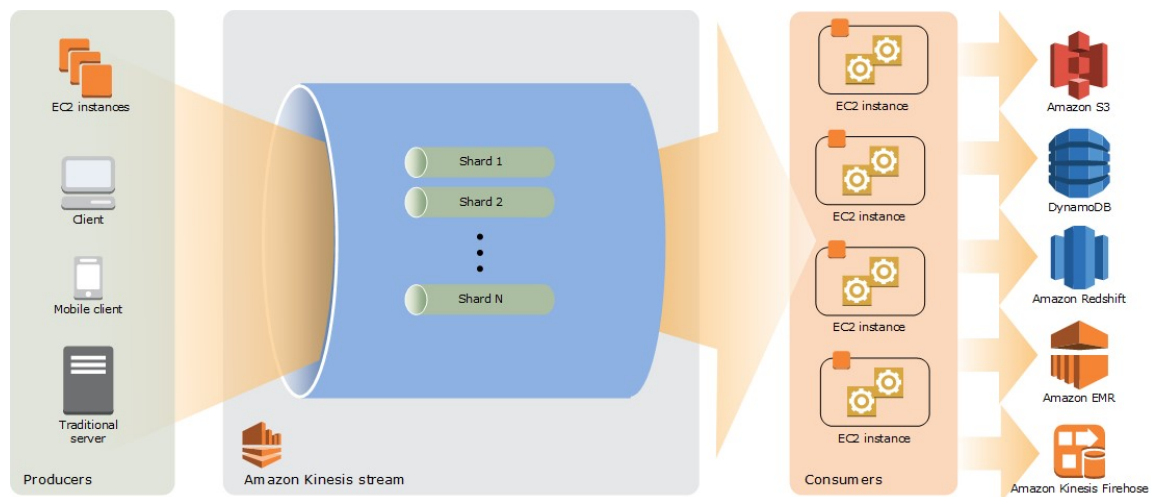
Answer – B

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 19

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You currently have a placement group of instances. When you try to add new instances to the group, you receive a 'capacity error'. Which of the following actions will most likely fix this problem? Choose the correct option from the below:

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

Explanation :

Answer – B

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

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

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

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

More information on Cluster Placement Group

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

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

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

Ask our Experts



QUESTION 20

UNATTEMPTED

DATA STORAGE

An International company has deployed a multi-tier web application that relies on DynamoDB in a single region. For regulatory reasons they need disaster recovery capability in a separate region with a Recovery Time Objective of 2 hours and a Recovery Point Objective of 24 hours. They should synchronize their data on a regular basis and be able to provision a web application rapidly

using CloudFormation. The objective is to minimize changes to the existing web application, control the throughput of DynamoDB used for the synchronization of data and synchronize only the modified elements.

Which design would you choose to meet these requirements?

- ☐ A. Use AWS Data Pipeline to schedule a DynamoDB cross region copy once a day, create a “Last updated” attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter.
- ☐ B. Use EMR and write a custom script to retrieve data from DynamoDB in the current region using a SCAN operation and push it to DynamoDB in the second region.
- ☐ C. Use AWS data pipeline to schedule an export of the DynamoDB table to S3 in the current region once a day then schedule another task immediately after it that will import data from S3 to DynamoDB in the other region. ✓
- ☐ D. Send each item into an SQS queue in the second region; use an auto-scaling group behind the SQS queue to replay the write in the second region.

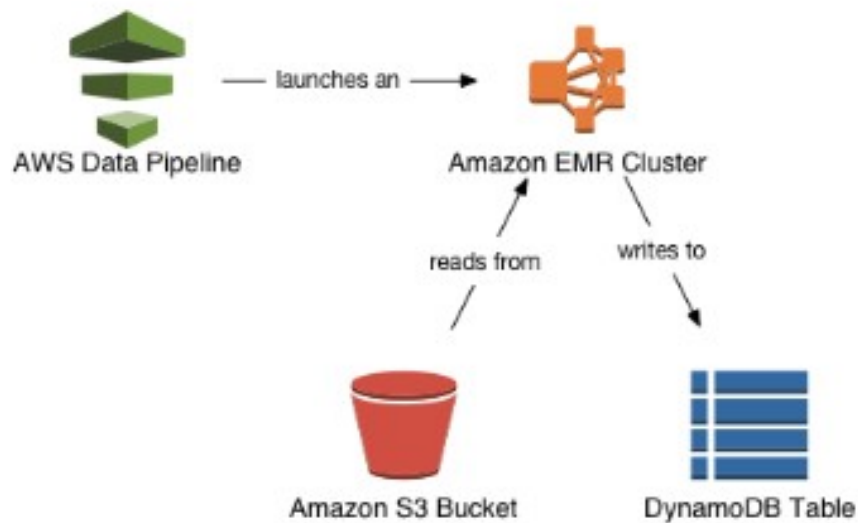
Explanation :

Answer - C

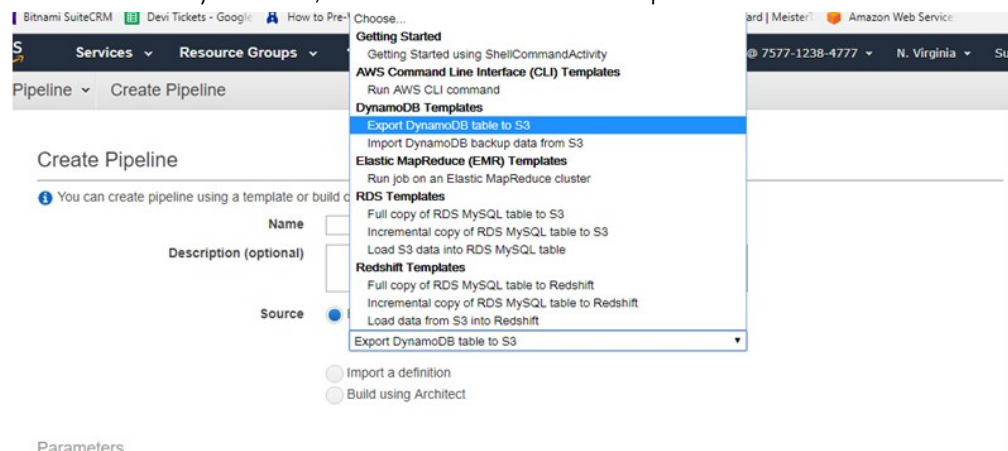
Exporting and Importing DynamoDB Data Using AWS Data Pipeline:

You can use AWS Data Pipeline to export data from a DynamoDB table to a file in an Amazon S3 bucket. You can also use the console to import data from Amazon S3 into a DynamoDB table, in the same AWS region or in a different region.

Importing Data from Amazon S3 to DynamoDB

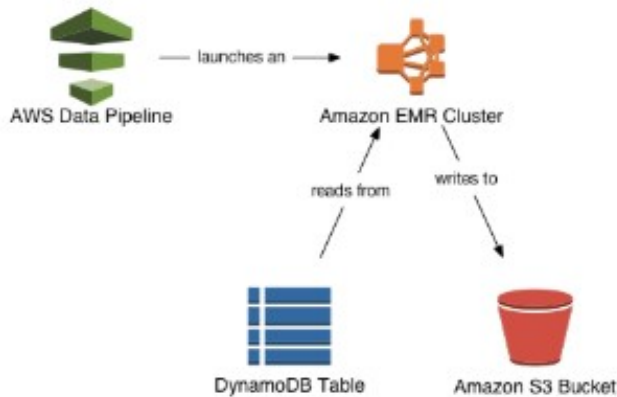


To export a DynamoDB table, you use the AWS Data Pipeline console to create a new pipeline. The pipeline launches an Amazon EMR cluster to perform the actual export. Amazon EMR reads the data from DynamoDB, and writes the data to an export file in an Amazon S3 bucket.



The process is similar for an import, except that the data is read from the Amazon S3 bucket and written to the DynamoDB table.

Exporting Data from DynamoDB to Amazon S3



Note: The question says "An International company has deployed a multi-tier web application that relies on DynamoDB in a **single region**."

So, we need to think in this point of view. And AWS exam is checking whether you have the understanding of the services and what can be done. And we need to find the best answer based on given option. In that way, though cross region feature is there, no need to discuss with that.

Please check the below link to know more about sync the data to S3.

- <https://aws.amazon.com/articles/using-dynamodb-with-amazon-elastic-mapreduce/>
(<https://aws.amazon.com/articles/using-dynamodb-with-amazon-elastic-mapreduce/>)

Ask our Experts



QUESTION 21

UNATTEMPTED

SECURITY

An auditor has been called upon to carry out an audit of the configuration of your AWS accounts. The auditor has specified that they just want to read only access to the AWS resources on all accounts. Which of the below options would help the auditor get the required access?

- ☐ A. Create an IAM user for each AWS account with read-only permission policies for the auditor, and disable each account when the audit is complete.

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

Explanation :

Answer – C

Option A is incorrect because creating an IAM User for each AWS account is an overhead and less preferred way compared to creating IAM Role.

Option B is incorrect because the scenario says that the company does not have any on-premises identity provider.

Option C is CORRECT because it creates an IAM Role which has all the necessary permission policies attached to it which allows the auditor to assume the appropriate role while accessing the resources.

Option D is incorrect because using the IAM Role that has the required permissions is the preferred and more secure way of accessing the AWS resources than using the Amazon credentials. Also, this option does not use any Security Token Service that gives temporary credentials to login. Hence this is a less secure way of accessing the AWS resources.

For more information on IAM roles please refer to the below URL

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

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

Ask our Experts



Currently, the developers in your organization have access to production AWS account. There is a concern raised that the developers could potentially delete the production-based EC2 resources. Which of the following options could help you to alleviate this concern?

Choose 2 options from the below:

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

Explanation :

Answer – A and B

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

Option A is CORRECT because it (a) identifies the instances with proper tag, and (b) creates a resource level permission and explicitly denies the user the terminate option.

Option B is CORRECT because it (a) identifies the instances with proper tag, and (b) creates a policy with explicit deny of terminating the instances and applies that policy to the group which contains the employees (who are not supposed to have the access to terminate the instances).

Option C and D are incorrect because MFA is an additional layer of security given to the users for logging into AWS and accessing the resources. However, either enabling or disabling MFA cannot prevent the users from performing resource level actions.

More information on Tags

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type – you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define.

For more information on tagging AWS resources please refer to the below URL

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

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

Ask our Experts



QUESTION 23

UNATTEMPTED

SCALABILITY & ELASTICITY

A legacy application is being migrated to AWS. It works on the TCP protocol. There is a requirement to ensure scalability of the application and also ensure that records of the client IP using the application are recorded.

Which of the below-mentioned steps would you implement to fulfill the above requirement?

- ☐ A. Use an ELB with a TCP Listener and Proxy Protocol enabled to distribute load on two or more application servers in different AZs. ✓
- ☐ B. Use an ELB with a TCP Listener and Cross-Zone Load Balancing enabled, two application servers in different AZs.
- ☐ C. Use Route 53 with Latency Based Routing enabled to distribute load on two or more application servers in different AZs.
- ☐ D. 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.

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>)

- (<https://aws.amazon.com/blogs/aws/elastic-load-balancing-adds-support-for-proxy-protocol/>)

Ask our Experts



QUESTION 24

UNATTEMPTED

SECURITY

Which of the following are the ways to minimize the attack surface area as a DDOS minimization strategy in AWS?

Choose 3 options from the below:

- ☐ A. Configure services such as Elastic Load Balancing and Auto Scaling to automatically scale.
- ☐ B. Reduce the number of necessary Internet entry points. ✓
- ☐ C. Use Amazon API Gateway as a “front door” to applications running on Amazon EC2 and AWS Lambda. ✓
- ☐ D. Eliminate non-critical Internet entry points. ✓

Explanation :

Answer – B, C, and D

Some important consideration when architecting on AWS is to limit the opportunities that an attacker may have to target your application. For example, if you do not expect an end user to directly interact with certain resources you will want to make sure that those resources are not accessible from the Internet. Similarly, if you do not expect end-users or external applications to communicate with your application on certain ports or protocols, you will want to make sure that traffic is not accepted. This concept is known as attack surface reduction.

Option A is incorrect because it is used for mitigating the DDoS attack where the system scales to absorb the application layer traffic in order to keep it responsive.

Option B, D are CORRECT as they all are used for reducing the DDoS attack surface.

Option C is correct. Typically, when you must expose an API to the public, there is a risk that the API frontend could be targeted by a DDoS attack. To help reduce the risk, you can use Amazon API Gateway as a “front door” to applications running on Amazon EC2, AWS Lambda, or elsewhere. By using Amazon API Gateway, you don’t need your own servers for the API frontend and you can obfuscate other components of your application. By making it harder to detect your application’s components, you can help prevent those AWS resources from being targeted by a DDoS attack.

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

(https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf)

For more information on DDoS attacks in AWS, please visit the below URL

https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

(https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf)

Ask our Experts



QUESTION 25

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You've created a temporary application that accepts image uploads, stores them in S3, and records the information about the images in RDS. After building this architecture and accepting the images for the duration required, it's time to delete the CloudFormation stack. However, your manager has informed you that, for some reason, they need to ensure that a backup is taken of the RDS when the CloudFormation stack is deleted. Which of the options below will fulfill the above requirement?

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

Explanation :

Answer - C

The main point in this scenario is that even if the CloudFormation stack is deleted there should be a way to be able to restore the RDS data if needed.

- Option A is incorrect because the DeletionPolicy of the RDS instance should be set to snapshot. If delete is used, the resource would get deleted and the data cannot be restored in the future.
- Option B is incorrect because DeletionPolicy attribute for RDS should be snapshot, not retain because with snapshot option, the backup of the RDS instance would be stored in the form of snapshots (which is the requirement). With retain option, CF will keep the RDS instance alive which is unwanted. There is such no requirement on S3.
- Option C is CORRECT because it correctly sets the DeletionPolicy of the RDS to snapshot so that the data can be restored from the snapshot if needed.

- Option D is incorrect because it sets the DeletionPolicy of the RDS to retain which will keep the RDS instance alive. It just needs to take the snapshot.

More information on DeletionPolicy on CloudFormation

DeletionPolicy options include:

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

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

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

For more information on Cloudformation deletion policy, please visit the below URL

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

Ask our Experts



QUESTION 26

UNATTEMPTED

SECURITY

An application, basically a mobile application needs access for each user to store data in a DynamoDB table. What is the best method for granting each mobile device that ensures the application has access DynamoDB tables for storage when required?

Choose the correct options from the below:

- ☐ A. During the install and game configuration process, have each user create an IAM credential and assign the IAM user to a group with proper permissions to communicate with DynamoDB.
- ☐ B. Create an IAM group that 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

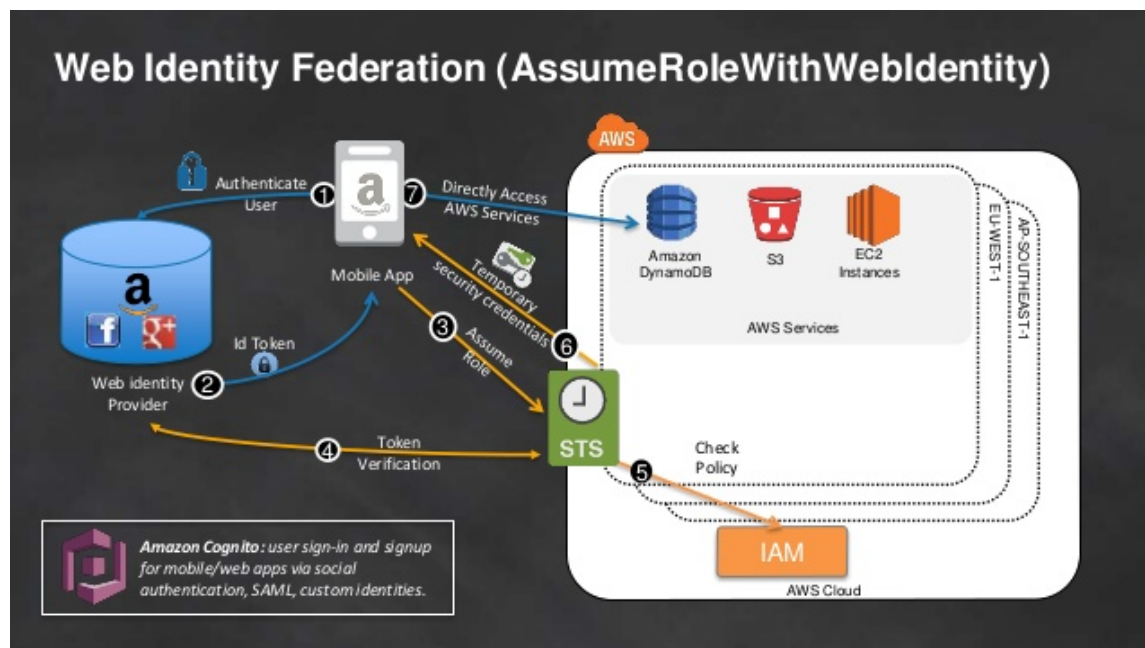
Option A is incorrect because IAM Roles are preferred over IAM Users, because IAM Users have to access the AWS resources using access and secret keys, which is a security concern.

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



QUESTION 27

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

A company has a Direct Connect established between their on-premise location and AWS. The applications hosted on the on-premise location are experiencing high latency when using S3. What could be done to ensure that the latency to S3 can be reduced?

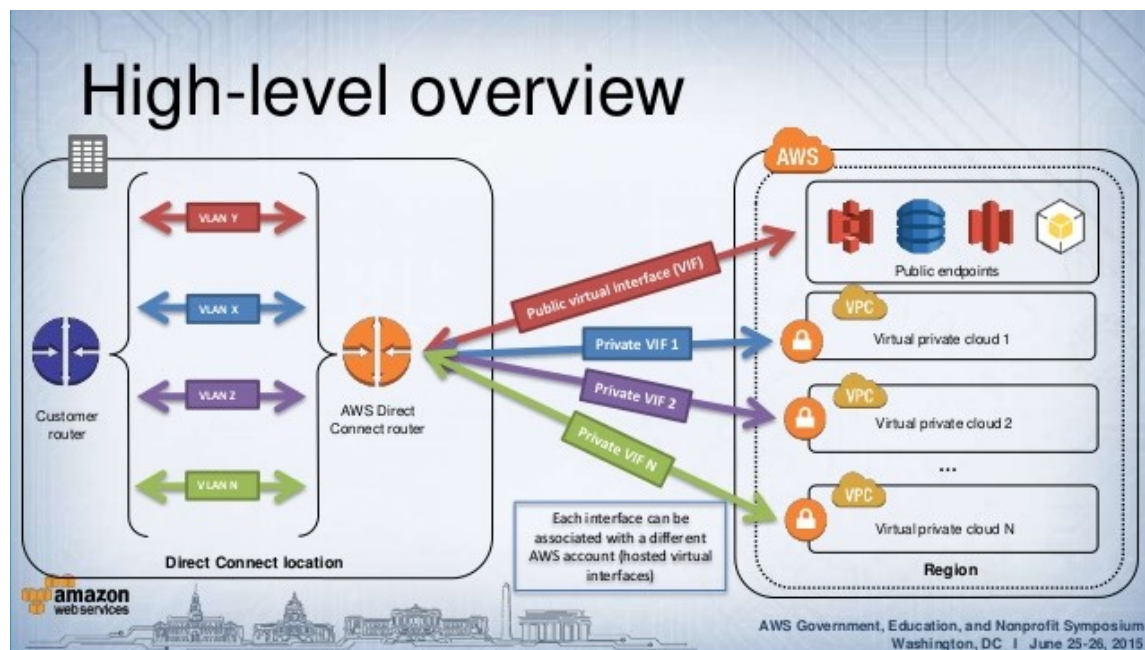
- ☐ A. Configure a public virtual interface to connect to a public S3 endpoint resource via Direct Connect connection. ✓
- ☐ B. Establish a VPN connection from the VPC to the public S3 endpoint.

- ☐ C. Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.
- ☐ D. Add a BGP route as part of the on-premise router; this will route S3 related traffic to the public S3 endpoint to dedicated AWS region.

Explanation :

Answer – A

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



Option A is CORRECT because, as mentioned above, it creates a public virtual interface to connect to S3 endpoint.

Option B is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not VPN.

Option C is incorrect because to connect to S3 endpoint, a public virtual interface needs to be created, not private.

Option D is incorrect because this setup will not help connecting to the S3 endpoint.

For more information on virtual interfaces, please visit the below URL

<http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>

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

Ask our Experts



QUESTION 28

UNATTEMPTED

DEPLOYMENT MANAGEMENT

There is a requirement to carry out the backup of an Oracle RAC cluster which is currently hosted on the AWS public cloud. How can this be achieved?

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

Explanation :

Answer – C

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

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

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

<https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/>
(<https://aws.amazon.com/about-aws/whats-new/2015/11/self-managed-oracle-rac-on-ec2/>)
<https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/>

(<https://aws.amazon.com/articles/oracle-rac-on-amazon-ec2/>)
(<https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/>)
(<https://aws.amazon.com/blogs/database/amazon-aurora-as-an-alternative-to-oracle-rac/>)

Ask our Experts



QUESTION 29

UNATTEMPTED

SECURITY

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

Choose the correct option from the below:

- ☐ A. Configure the RDS instance as the master and enable replication over the open internet using a secure SSL endpoint to the on-premise server.
- ☐ B. RDS cannot replicate to an on-premise database server. Instead, first configure the RDS instance to replicate to an EC2 instance with core MySQL, and then configure replication over a secure VPN/VPG connection.
- ☐ C. Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint.
- ☐ D. 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.

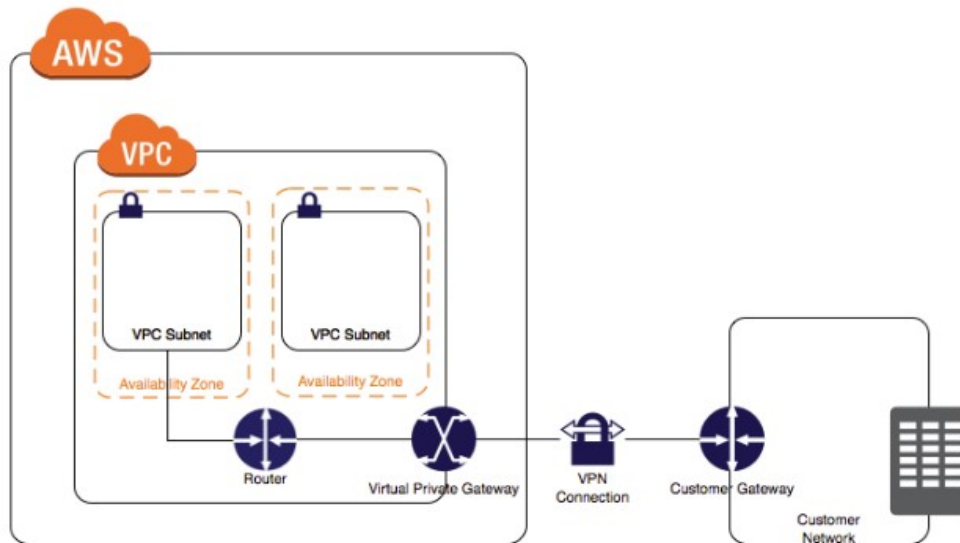
Option B is incorrect because replicating via EC2 instances is very time consuming and very expensive cost-wise.

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 30

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company's on-premises content management system has the following architecture:

Application Tier – Java code on a JBoss application server

Database Tier – Oracle database regularly backed up to Amazon Simple Storage Service (S3) using the Oracle RMAN backup utility

Static Content – stored on a 512GB gateway stored Storage Gateway volume attached to the application server via the iSCSI interface

Which AWS based disaster recovery strategy will give you the best RTO?

- ☐ A. Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Generate an EBS volume of static content from the Storage Gateway and attach it to the JBoss EC2 server. ✓
- ☐ B. Deploy the Oracle database on RDS. Deploy the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon Glacier. Generate an EBS volume of static content from the Storage Gateway and attach it to the JBoss EC2 server.
- ☐ C. Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Restore the static content by attaching an AWS Storage Gateway running on Amazon EC2 as an iSCSI volume to the JBoss EC2 server.
- ☐ D. Deploy the Oracle database and the JBoss app server on EC2. Restore the RMAN Oracle backups from Amazon S3. Restore the static content from an AWS Storage Gateway-VTL running on Amazon EC2

Explanation :

Answer - A

Option A is CORRECT because (i) it deploys the Oracle database on EC2 instance by restoring the backups from S3 which is quick, and (ii) it generates the EBS volume of static content from Storage Gateway. Due to these points, option A meet the best RTO compared to all the remaining options.

Option B is incorrect because restoring the backups from the Amazon Glacier will be slow and will not meet the RTO.

Option C is incorrect because there is no need to attach the Storage Gateway as an iSCSI volume; you can just easily and quickly create an EBS volume from the Storage Gateway. Then you can generate snapshots from the EBS volumes for better recovery time.

Option D is incorrect as restoring the content from Virtual Tape Library will not fit into the RTO.

Ask our Experts



An ERP application is deployed in multiple Availability Zones in a single region. In the event of failure, the RTO must be less than 3 hours and the RPO is 15 minutes. The customer realizes that data corruption occurred roughly 1.5 hours ago. Which DR strategy can be used to achieve this RTO and RPO in the event of this kind of failure?

- ☐ A. Take 15-minute DB backups stored in Amazon Glacier, with transaction logs stored in Amazon S3 every 5 minutes.
- ☐ B. Use synchronous database master-slave replication between two Availability Zones.
- ☒ C. Take hourly DB backups to Amazon S3, with transaction logs stored in S3 every 5 minutes. ✓
- ☐ D. Take hourly DB backups to an Amazon EC2 instance store volume, with transaction logs stored in Amazon S3 every 5 minutes.

Explanation :

Answer - C

Option A is incorrect because restoring the backups from Amazon Glacier would be slow and will definitely not meet the RTO and RPO.

Option B is incorrect because with the synchronous replication you cannot go back to point in time recovery. You will always have the latest data.

Option C is CORRECT because it takes hourly backups to Amazon S3 - which makes restoring the backups quick, and since the transaction logs are stored in S3 every 5 minutes, it will help to restore the application to a state that is within the RPO of 15 minutes.

Option D is incorrect because instant store volume is ephemeral. i.e. the data can get lost when the instance is terminated.

NOTE:

Although Glacier supports expedited retrieval (On-Demand and Provisioned), it is an expensive option and is recommended only for occasional urgent request for a small number of archives. Having said this (and even if we go with glacier as solution), the option also mentions taking database snapshots every 15 minutes. Now if you keep taking backups every 15 mins, the database users are going to face lot of outages during the backup (due to I/O suspension especially in non-AZ deployment). Also, within 15 minutes the backup process may not even finish!

As an architect you need to use the database change (transaction) logs along with the backups to restore your database to a point in time. Since option (c) stores the transaction details up to last 5 minutes, you can easily restore your database and meet the RPO of 15 minutes. Hence, C is the best choice.

Ask our Experts



QUESTION 32

UNATTEMPTED

COSTING

The Marketing Director in your company asked you to create a mobile app that lets users post sightings of good deeds known as random acts of kindness in 80-character summaries. You decided to write the application in JavaScript so that it would run on the broadest range of phones, browsers, and tablets. Your application should provide access to Amazon DynamoDB to store the good deed summaries. Initial testing of a prototype shows that there aren't large spikes in usage. Which option provides the most cost-effective and scalable architecture for this application?

- ☐ A. Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) on an EC2 instance to provide signed credentials mapped to an Amazon Identity and Access Management (IAM) user allowing DynamoDB puts and S3 gets. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB.
- ☐ B. Register the application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow S3 gets and DynamoDB puts. You serve your mobile application out of an S3 bucket enabled as a web site. Your client updates DynamoDB. ✓

- ☐ C. Provide the JavaScript client with temporary credentials from the Security Token Service using a Token Vending Machine (TVM) to provide signed credentials mapped to an IAM user allowing DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB.
- ☐ D. Register the JavaScript application with a Web Identity Provider like Amazon, Google, or Facebook, create an IAM role for that provider, and set up permissions for the IAM role to allow DynamoDB puts. You serve your mobile application out of Apache EC2 instances that are load-balanced and autoscaled. Your EC2 instances are configured with an IAM role that allows DynamoDB puts. Your server updates DynamoDB.

Explanation :

Answer – B

This scenario asks to design a cost-effective and scalable solution where a multi-platform application needs to communicate with DynamoDB. For such scenarios, federated access to the application is the most likely solution.

Option A is incorrect because the Token Vending Machine (STS Service) is implemented on a single EC2 instance which is a single point of failure. This is not a scalable solution either as the instance can become the performance bottleneck.

Option B is CORRECT because, (i) it authenticates the application via federated identity provider such as Amazon, Google, Facebook etc, (ii) it sets up the proper permission for DynamoDB access, and (iii) S3 website which supports Javascript - is a highly scalable and cost effective solution.

Option C is incorrect because deploying EC2 instances in auto-scaled environment is not as cost-effective solution as the S3 website, even though it is scalable.

Option D is incorrect because it is suggesting to run the website on an Autoscaling group of EC2 instances with an ELB in the front end. This option is not the most cost effective solution provided. Hence this is invalid.

Ask our Experts



You are building a website that will retrieve and display highly sensitive information to users. The amount of traffic the site will receive is known and not expected to fluctuate. The site will leverage SSL to protect the communication between the clients and the web servers. Due to the nature of the site you are very concerned about the security of your SSL private key and want to ensure that the key cannot be accidentally or intentionally moved outside your environment. Additionally, while the data the site will display is stored on an encrypted EBS volume, you are also concerned that the web servers' logs might contain some sensitive information; therefore, the logs must be stored so that they can only be decrypted by employees of your company. Which of these architectures meets all of the requirements?

- ☐ A. Use Elastic Load Balancing to distribute traffic to a set of web servers. To protect the SSL private key, upload the key to the load balancer and configure the load balancer to offload the SSL traffic. Write your web server logs to an ephemeral volume that has been encrypted using a randomly generated AES key.
- ☐ B. Use Elastic Load Balancing to distribute traffic to a set of web servers. Use TCP load balancing on the load balancer and configure your web servers to retrieve the private key from a private Amazon S3 bucket on boot. Write your web server logs to a private Amazon S3 bucket using Amazon S3 server-side encryption.
- ☐ C. Use Elastic Load Balancing to distribute traffic to a set of web servers, configure the load balancer to perform TCP load balancing, use an AWS CloudHSM to perform the SSL transactions, and write your web server logs to a private Amazon S3 bucket using Amazon S3 server-side encryption. ✓
- ☐ D. Use Elastic Load Balancing to distribute traffic to a set of web servers. Configure the load balancer to perform TCP load balancing, use an AWS CloudHSM to perform the SSL transactions, and write your web server logs to an ephemeral volume that has been encrypted using a randomly generated AES key.

Explanation :

Answer – C

Option A and D both are incorrect because the logs - which contain the sensitive information - are written to ephemeral volume. So there are chances that the data can get lost upon termination of the EC2 instance.

Option B is incorrect because it does not use a secure way of managing the SSL private key for SSL transaction.

Option C is CORRECT because it uses CloudHSM for performing the SSL transaction without requiring any additional way of storing or managing the SSL private key. This is the most secure way of ensuring that the key will not be moved outside of the AWS environment. Also, it uses the highly available and durable S3 service for storing the logs.

More information on AWS CloudHSM:

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM.

For more information on AWS CloudHSM, please refer to the link:

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

Ask our Experts



QUESTION 34

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

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

- ☐ A. Use S3 with reduced redundancy to store and serve the scanned files. Install a 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 scanned files with a search index.
- ☐ C. Use S3 with standard redundancy 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 scanned files and use an EC2 instance with a custom application to search based on the index.

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 its end of life, (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 its end of life.

Option B is incorrect because striped EBS is not as durable 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, (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.

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

You are designing network connectivity for your fat client application. The application is designed for business travelers who must be able to connect to it from their hotel rooms, cafes, public Wi-Fi hotspots, and elsewhere on the Internet. While you do not want to publish the application on the Internet.

Which network design meets the above requirements while minimizing deployment and operational costs? Choose the correct answer from the options below

- ☐ A. Implement AWS Direct Connect, and create a private interface to your VPC. Create a public subnet and place your application servers in it.
- ☐ B. Implement Elastic Load Balancing with an SSL listener that terminates the back-end connection to the application.
- ☐ C. Configure an IPsec VPN connection, and provide the users with the configuration details. Create a public subnet in your VPC, and place your application servers in it.

- ☐ D. Configure an SSL VPN solution in a public subnet of your VPC, then install and configure SSL VPN client software on all user computers. Create a private subnet in your VPC and place your application servers in it. ✓

Explanation :

Answer – D

Option A is incorrect because AWS Direct Connect is not a cost effective solution compared to using VPN solution.

Option B is incorrect because it does not mention how the application would be accessible only to the business travelers and not to the public.

Option C is incorrect because if the application servers are put in the public subnet, they would be publicly accessible via the internet.

Option D is CORRECT because configuring the SSL VPN solution is cost-effective and allows access only to the business travelers and since the application servers are in private subnet, the application is not accessible via the internet.

Ask our Experts



QUESTION 36

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Which of the below components is used by AWS Data Pipeline to poll for tasks and then performs those tasks?

- ☐ A. Definition Syntax File
- ☐ B. S3
- ☐ C. Task Runner ✓
- ☐ D. AWS OpsWork

Explanation :

Answer - C

Task Runner is a task agent application that polls AWS Data Pipeline for scheduled tasks and executes them on Amazon EC2 instances, Amazon EMR clusters, or other computational resources, reporting status as it does so.

For more information on the Taskrunner in AWS pipeline, please refer to the below link
<http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-using-task-runner.html>
(<http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-using-task-runner.html>)

Ask our Experts



QUESTION 37

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

An organization has created multiple components of a single application. Currently, all the components are hosted on a single EC2 instance. Due to security reasons, the organization wants to implement 2 separate SSL certificates for the separate modules.

How can the organization achieve this with a single instance?

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

Explanation :

Answer - A

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

- (1) Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address.
- (2) Operate network appliances, such as firewalls or load balancers, that have multiple IP

addresses for each network interface.

(3) Redirect internal traffic to a standby instance in case your instance fails, by reassigning the secondary IP address to the standby instance.

Option A is CORRECT because, as mentioned above, if you have multiple elastic network interfaces (ENIs) attached to the EC2 instance, each network IP can have a component running with a separate SSL certificate.

Option B is incorrect because having separate rules in security group as well as NACL does not mean that the instance supports multiple SSLs.

Option C is incorrect because an EC2 instance cannot have multiple subnets.

Option D is incorrect because NAT address is not related to supporting multiple SSLs.

For more information on Multiple IP Addresses, please refer to the link below:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html>

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

Ask our Experts



QUESTION 38

UNATTEMPTED

NETWORK DESIGN

A company has configured and peered two VPCs: VPC-1 and VPC-2. The VPC-1 contains only private subnets, and VPC-2 contains only public subnets. The company uses a single AWS Direct Connect connection and private virtual interface to connect their on-premises network with VPC-1. Which two methods increase the fault tolerance of the connection to VPC-1? Choose 2 answers:

- ☐ A. Establish a hardware VPN over the internet between VPC-2 and the on-premises network.
- ☐ B. Establish a hardware VPN over the internet between VPC-1 and the on-premises network. ✓
- ☐ C. Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.
- ☐ D. Establish a new AWS Direct Connect connection and private virtual interface in a different AWS region than VPC-1.

- ☐ E. Establish a new AWS Direct Connect connection and private virtual interface in the same AWS region as VPC-1. ✓

Explanation :

Answer - B & E

Option A & C are incorrect because peered VPC does not support Edge-to-Edge Routing, so connecting to VPC2 will not work.

Option B is CORRECT because hardware VPN can be created to connect the VPC-1 with the on-premises network.

Option D is incorrect because AWS Direct Connect is a regional service and you cannot reach VPC1 if the direct connect is in a different region.

Option E is CORRECT because AWS Direct Connect is a regional service and will work if it is in the same region as that of the VPC-1.

For more information on VPC peering, please see the links below:

<https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html> (<https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/invalid-peering-configurations.html>)

Ask our Experts



QUESTION 39

UNATTEMPTED

NETWORK DESIGN

Your company produces customer commissioned one-of-a-kind skiing helmets combining high fashion with custom technical enhancements. Customers can show off their individuality on the ski slopes and have access to head-up-displays, GPS rear-view cams and any other technical innovation they wish to embed in the helmet. 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 the automated assessments. You need to add a new set of assessment to model the failure modes of the

electronics using GPUs with CUDA 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 autoscaling group of G2 instances in a placement group.
- ☐ B. Use Amazon Simple Workflow (SWF) to manage assessments, movement of data & meta-data. Use an auto-scaling group of G2 instances in a placement group. ✓
- ☐ C. Use Amazon Simple Workflow (SWF) to manage assessments movement of data & meta-data. Use an auto-scaling 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 autoscaling group of C3 with SR-IOV (Single Root I/O virtualization).

Explanation :

Answer - B

The main point to consider in this question is that the assessments include human interaction as well. In most of such cases always look for SWF in the options.

Option A is incorrect because this will be useful during the batch jobs which deal with the automated assessments. For the human assessment, this will not be a useful option.

Option B is CORRECT because (a) it enables assessment via human interaction, (b) uses autoscaled G2 instances that are efficient in automated assessments due to their GPU and low latency networking.

Option C is incorrect because, C3 instances and SR-IOV will not provide required GPU.

Option D is incorrect because, (a) this will be useful during the batch jobs which deal with the automated assessments. For the human assessment, this will not be a useful option, and (b) C3 instances and SR-IOV will not provide required GPU.



QUESTION 40

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A web company is looking to implement an external payment service into their highly available application deployed in a VPC. Their application EC2 instances are behind a public facing ELB. Auto scaling is used to add additional instances as traffic increases under normal load. The application runs 2 instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisting IP addresses are allowed at a time and can be added through an API. How should they architect their solution?

- ☒ **A. Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the NAT instances.**
✓
- ☐ **B. Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway.**
- ☐ **C. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.**
- ☐ **D. Automatically assign public IP addresses to the application instances in the Auto Scaling group and run a script on boot that adds each instances public IP address to the payment validation whitelist API.**

Explanation :

Answer - A

Option A is CORRECT because (a) the requests originated from the instances in the subnet would be routed through the NAT, so the requests would have the NAT's IP address (which is whitelisted), and (b) two NAT instances would provide high availability.

Option B is incorrect because (a) Internet Gateway (IGW) can only route the traffic, it cannot whitelist any particular IP and payment requests, and (b) EC2 instances with public IP addresses in a public subnet are routed through the gateway, but will keep their own IP address, so they will not get whitelisted.

Option C is incorrect because the outbound traffic cannot be routed through an ELB.

Option D is incorrect because, the ASG will have 6 servers during the peak load, and the payment service only allows 4 to be whitelisted; so, it will exceed the allowed 4 IP addresses.

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

Ask our Experts



QUESTION 41

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Which of the following AWS services can be used to define alarms to trigger on a certain activity in the AWS Data pipeline?

- ☒ A. SNS ✓
- ☐ B. SQS
- ☐ C. SES
- ☐ D. CodeDeploy

Explanation :

Answer - A

Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push notification service that lets you send individual messages or to fan-out messages to large numbers of recipients. Amazon SNS makes it simple and cost effective to send push notifications to mobile device users, email recipients or even send messages to other distributed services.

For more information on SNS, please refer to the below link
<https://aws.amazon.com/sns/> (<https://aws.amazon.com/sns/>)

Note:

For AWS Pipeline, you can use SNS to notify you the alerts without Cloudwatch.

AWS says that "AWS Data Pipeline actions are steps that a pipeline component takes when certain events occur, such as success, failure, or late activities. The event field of an activity refers to an action, such as a reference to *snsAlarm* in the *onLateAction* field of *EmrActivity*.

AWS Data Pipeline relies on Amazon SNS notifications as the primary way to indicate the status of pipelines and their components in an unattended manner. For more information, see Amazon SNS (<https://aws.amazon.com/sns/>). In addition to SNS notifications, you can use the AWS Data Pipeline console and CLI to obtain pipeline status information."

Please check the below link to know more about it.

<https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-concepts-actions.html>
(<https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-concepts-actions.html>)

Ask our Experts



QUESTION 42

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Your company currently has a 2-tier web application running in an on-premises data center. You have experienced several infrastructure failures in the past two months resulting in significant financial losses. Your CIO is strongly agreeing to move the application to AWS. While working on achieving buy-in from the other company executives, he asks you to develop a disaster recovery plan to help improve Business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks. Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?

- ☐ A. Create an EBS backed private AMI which includes a fresh install of your application. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying the application across Multiple- Availability-Zones. Asynchronously replicate the transactions from your on-premises database to a database instance in AWS across a secure VPN connection. ✓
- ☐ B. Deploy your application on EC2 instances within an Auto Scaling group across multiple availability zones. Asynchronously replicate the transactions from your on-premises database to a database instance in AWS across a secure VPN connection.
- ☐ C. Create an EBS backed private AMI which includes a fresh install of your application. Setup a script in your data center to backup the local database every 1 hour and to encrypt and copy the resulting file to an S3 bucket using multi-part upload.
- ☐ D. Install your application on a compute-optimized EC2 instance capable of supporting the application's average load. Synchronously replicate the transactions from your on-premises database to a database instance in AWS across a secure Direct Connect connection.

Explanation :

Answer - A

Option A is CORRECT because (a) with AMIs, the newly created EC2 instances will be ready with the pre-installed application; thus, reducing the RTO, (b) with CloudFormation, the entire stack can be automatically provisioned, and (c) since there are no additional services used, the cost will stay low.

Option B is incorrect because although this could work, (a) deploying EC2 instances for this scenario will be expensive, and (b) in case of disaster, the recovery will potentially be slower, since the new EC2 need to be manually updated with the application software and patches, especially since it does not use the AMIs.

Option C is incorrect because it has a low performance issue. (a) Backing up local DB of 200GB on a 20Mbps connection every hour will be very slow, and (b) even with the incremental backup, recovering from the incremental backup take times and might not satisfy the given RTO.

Option D is incorrect because (a) the EC2 instance is a single point of failure, which needs to be made highly available via an autoscaling, and (b) it can only handle the average load of the application; so, in case of peak load, it may fail, and (c) AWS Direct Connection will be an expensive solution compared to the setup of option A.

Ask our Experts



QUESTION 43

UNATTEMPTED

NETWORK DESIGN

An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the web server on a single EC2 instance such that it allows the internet traffic as well as the back-end management traffic. The organization wants to make sure that the back end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing web server will have an IP address which can receive traffic from all the internet IPs.

How can the organization achieve this by running the web server on a single instance?

- ☐ A. It is not possible to have 2 IP addresses for a single instance
- ☐ B. The organization should create 2 network interfaces, one for the internet traffic and the other for the backend traffic ✓
- ☐ C. The organization should create 2 EC2 instances as this is not possible with one EC2 instance
- ☐ D. This is not possible

Explanation :

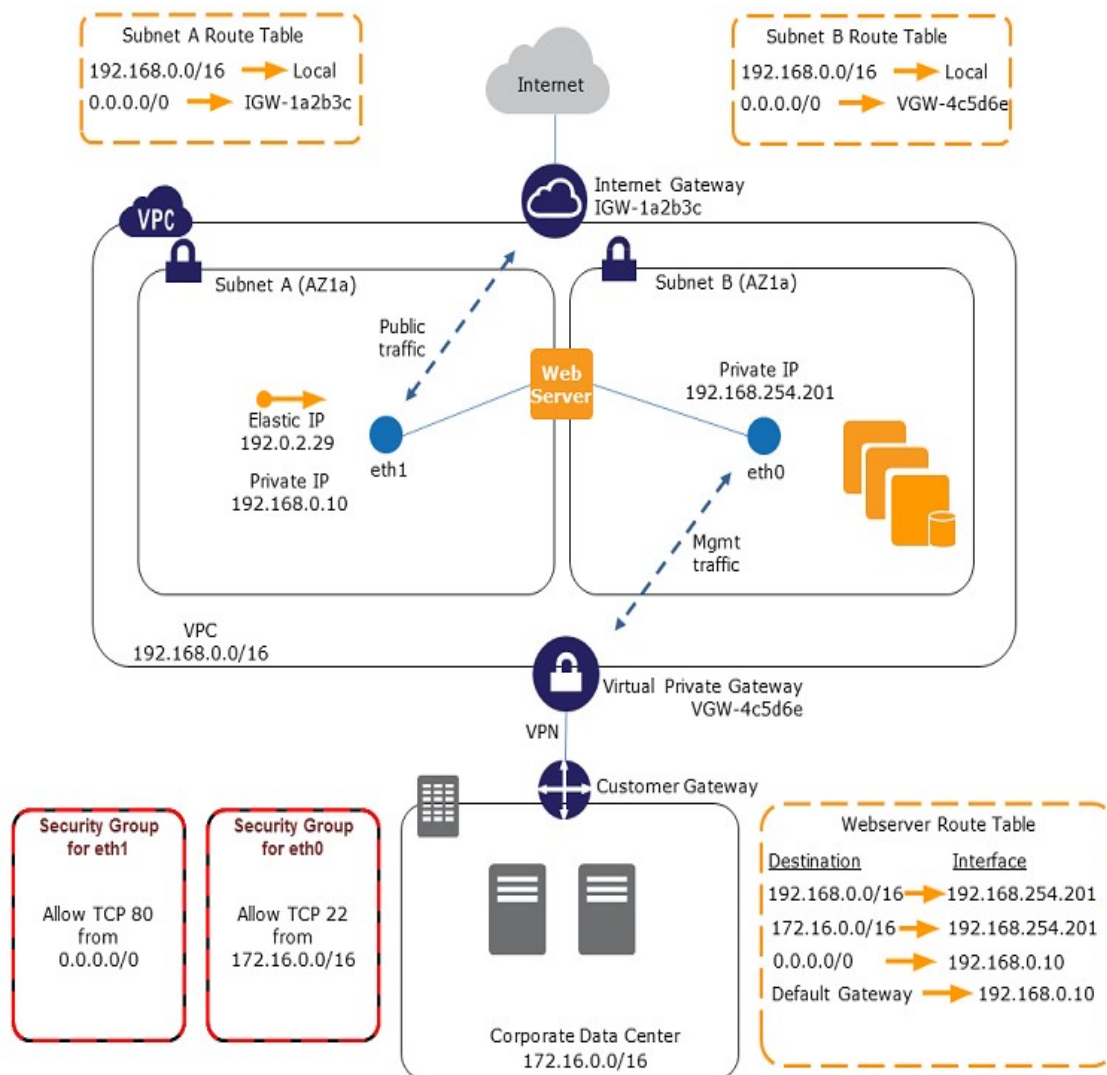
Answer - B

An Elastic Network Interface (ENI) is a virtual network interface that you can attach to an instance in a VPC. Network interfaces are available only for instances running in a VPC.

A network interface can include the following attributes:

- A primary private IPv4 address
- One or more secondary private IPv4 addresses
- One Elastic IP address (IPv4) per private IPv4 address
- One public IPv4 address
- One or more IPv6 addresses
- One or more security groups
- A MAC address
- A source/destination check flag
- A description

See an example below how the route table can be configured to allow the IP based access via multiple ENIs.



For more information on ENI , please refer to the below link

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

Ask our Experts



QUESTION 44

UNATTEMPTED

COSTING

A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files. They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and keep the costs to a minimum.

What AWS architecture would you recommend?

- ☐ A. Ask their customers to use an S3 client instead of an FTP client. Create a single S3 bucket. Create an IAM user for each customer. Put the IAM Users in a Group that has an IAM policy that permits access to subdirectories within the bucket via use of the 'username' policy variable. ✓
- ☐ B. Create a single S3 bucket with Reduced Redundancy Storage turned on and ask their customers to use an S3 client instead of an FTP client. Create a bucket for each customer with a Bucket Policy that permits access only to that one customer.
- ☐ C. Create an auto-scaling group of FTP servers with a scaling policy to automatically scale-in when minimum network traffic on the auto-scaling group is below a given threshold. Load a central list of ftp users from S3 as part of the user data startup script on each Instance.

- ☐ D. Create a single S3 bucket with Requester Pays turned on and ask their customers to use an S3 client instead of an FTP client. Create a bucket for each customer with a bucket policy that permits access only to that one customer.

Explanation :

Answer - A

The main considerations in this scenario are: (1) the architecture should be scalable, (2) customer privacy should be maintained, and (3) the solution should be cost-effective.

Option A is CORRECT because (a) it creates permissions via IAM policy where each user will have access to only those subdirectory named with their username, and (b) S3 is a cost-effective and highly scalable solution.

Note: Even though creating one IAM User per user/customer is not the best way forwards, but given the other choices, this is the best option.

Option B is incorrect because even though it uses RRS which is a less expensive solution than S3, creating one bucket per user is not a scalable architecture. Currently, the number of customers is 250, but in future the number can grow and if it does, it will put limits on the number of buckets.

Option C is incorrect because creating auto-scaling group of FTP servers is a costly solution compared to creating buckets on S3 and appropriate IAM policies.

Option D is incorrect because (a) creating one bucket per user is not a scalable architecture. Currently, the number of customers is 250, but in future the number can grow and if it does, it will put limits on the number of buckets, and (b) you configure buckets to be Requester Pays when you want to share the data but not incur charges associated with others accessing the data. This will keep the cost down for the company, but will increase the cost for the customer who will access the buckets.

Ask our Experts



There is a requirement for an application hosted on a VPC to access the On-premise LDAP server and then access the data stored in a S3 bucket. The VPC and the on-premise location are connected via an IPsec VPN. Which of the below are the right options for the application to authenticate each user?

Choose 2 options from below.

- ☐ A. Develop an identity broker that authenticates against IAM security Token service 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.
- ☐ 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 to assume that IAM role. The application then uses the temporary credentials to access the appropriate resources in AWS. ✓
- ☐ C. Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials. The application calls the identity broker to get IAM federated user credentials with access to the appropriate AWS service. ✓
- ☐ 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 AWS service.

Explanation :

Answer – B and C

There are two architectural considerations here: (1) The users must be authenticate 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.

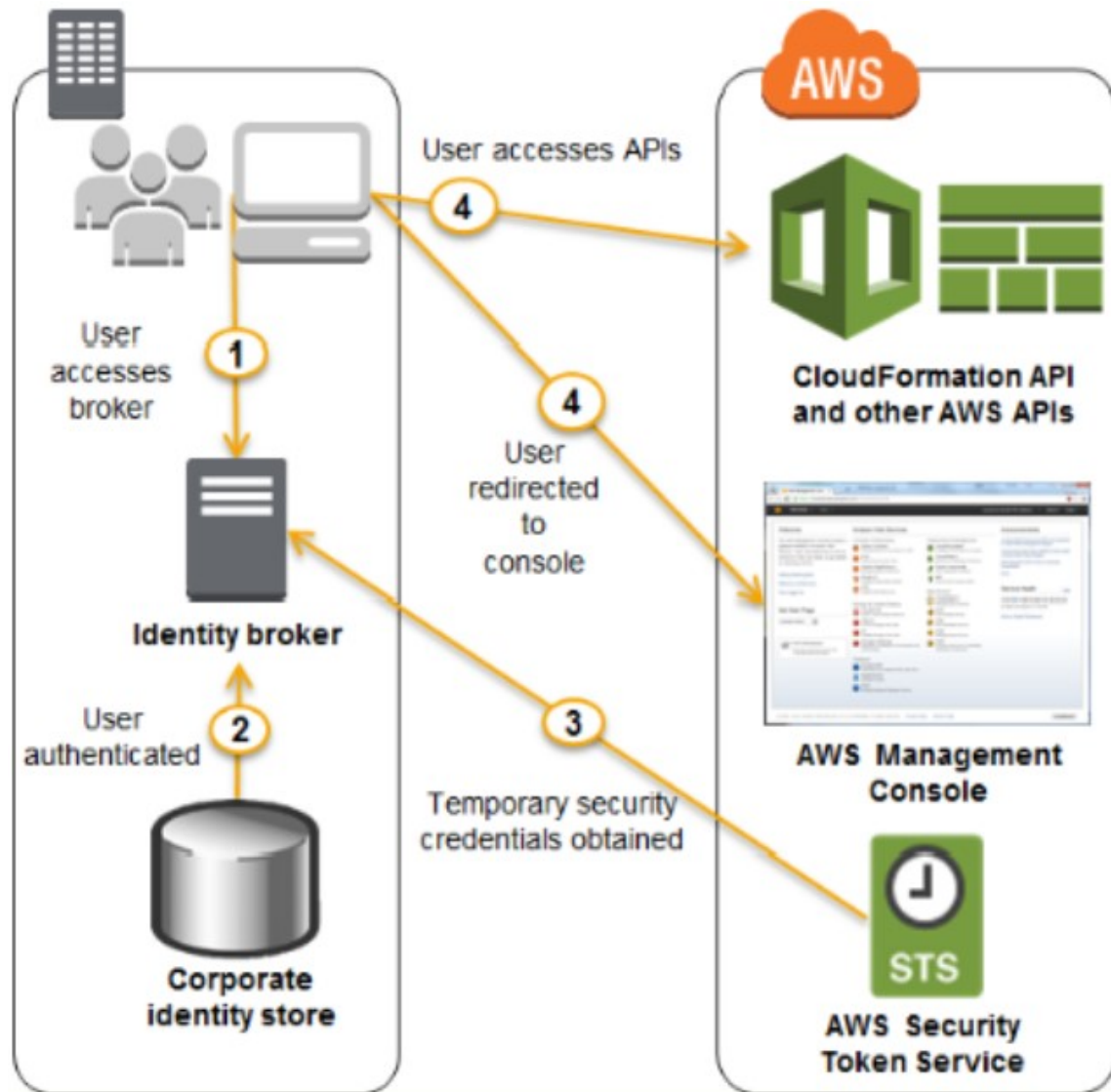
Option A is incorrect because the users need to be authenticated using LDAP first, not STS. Also, the temporary credentials to log into AWS are provided by STS, not identity broker.

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)

Ask our Experts



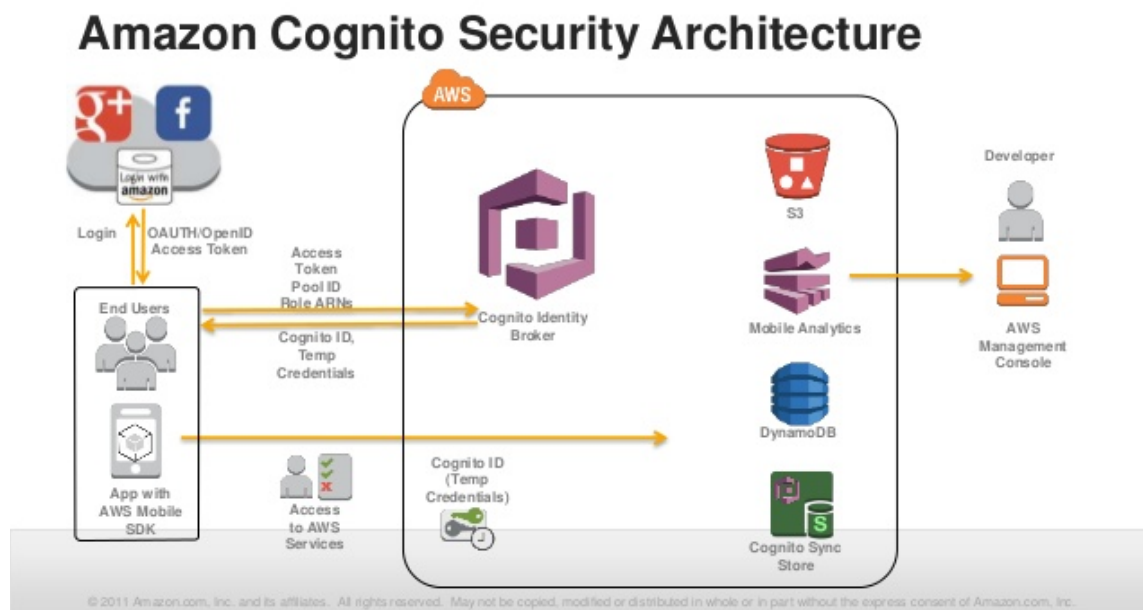
In Amazon Cognito, your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito. Which of the following is returned for the user to provide a set of temporary, limited-privilege AWS credentials?

- ☐ A. Cognito SDK
- ☐ B. Cognito Key pair
- ☒ C. Cognito Identity ID ✓
- ☐ D. Cognito API

Explanation :

Answer - C

If you're allowing unauthenticated users, you can retrieve a unique Amazon Cognito identifier (identity ID) for your end user immediately. If you're authenticating users, you can retrieve the identity ID after you've set the login tokens in the credentials provider



For more information on Cognito ID, please refer to the below link:

<http://docs.aws.amazon.com/cognito/latest/developerguide/getting-credentials.html>
(<http://docs.aws.amazon.com/cognito/latest/developerguide/getting-credentials.html>)

Ask our Experts



QUESTION 47

UNATTEMPTED

SCALABILITY & ELASTICITY

You have been asked to design network connectivity between your existing data centers and AWS. Your application's EC2 instances must be able to connect to existing backend resources located in your data center. Network traffic between AWS and your data centers will start small, but ramp up to 10s of GB per second over the course of several months. The success of your application is dependent upon getting to market quickly. Which of the following design options will allow you to meet your objectives?

- ☐ A. Quickly create an internal ELB for your backend applications, submit a Direct Connect request to provision a 1 Gbps cross connect between your data center and VPC, then increase the number or size of your Direct Connect connections as needed.
- ☐ B. Allocate EIPs and an Internet Gateway for your VPC instances to use for quick, temporary access to your backend applications, then provision a VPN connection between a VPC and existing on -premises equipment.
- ☐ C. Provision a VPN connection between a VPC and existing on-premises equipment, submit a Direct Connect partner request to provision cross connects between your data center and the Direct Connect location, then cut over from the VPN connection to one or more Direct Connect connections as needed. ✓
- ☐ D. Quickly submit a Direct Connect request to provision a 1 Gbps cross connect between your data center and VPC, then increase the number or size of your Direct Connect connections as needed.

Explanation :

Answer - C

The most important considerations in this scenario are: (1) the network traffic would be initially small, and will increase in future, and (2) the application should be up quickly, so time is critical. One thing should be noted that it takes time initially to set up the AWS Direct Connect (See the link below for latest information).

https://docs.aws.amazon.com/directconnect/latest/UserGuide/getting_started.html
(https://docs.aws.amazon.com/directconnect/latest/UserGuide/getting_started.html)

Option A is incorrect because setting up of Direct Connect will take time; so, the backend servers will not be connected in quick time.

Option B is incorrect because provisioning VPN only is not a long term solution since the traffic would increase to over 10Gbps.

Option C is CORRECT because (a) it provides quick connection between the on-premise data center and AWS via VPN, and (b) it also initiates the provision of a Direct Connect solution to tackle the requirement of higher bandwidth (for 10Gbps network) for later.

Option D is incorrect because setting up of Direct Connect will take time and the application will not be up within time as it is time critical.

For more information on VPN and Direct Connect, please visit the link below:

<https://datapath.io/resources/blog/aws-direct-connect-vs-vpn-vs-direct-connect-gateway/>
(<https://datapath.io/resources/blog/aws-direct-connect-vs-vpn-vs-direct-connect-gateway/>)

Ask our Experts



QUESTION 48

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Which of the following features ensures even distribution of traffic to Amazon EC2 instances in multiple Availability Zones registered with a load balancer?

- ☐ A. Elastic Load Balancing request routing
- ☐ B. An Amazon Route 53 weighted routing policy
- ☐ C. Elastic Load Balancing cross-zone load balancing ✓

☐ D. An Amazon Route 53 latency routing policy

Explanation :

Answer: C

Option A is incorrect because there is no request routing option available on ELB.

Option B is incorrect because Route 53 Weighted Routing will help resolving the DNS requests to different end points. Even though it is a DNS level load balancing, it will not help balancing the load on instances across multiple availability zones while being able to register/un-register instances based on the health check. That functionality is carried out by ELB.

Option C is CORRECT because you can enable the "Cross Zone Load Balancing" on ELB to even distribution of the traffic across instances in multiple AZs. See the image below:

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the

VPC vpc-6dcc550a (172.31.0.0/16)

<input type="checkbox"/>	Instance	Name
--------------------------	----------	------

Availability Zone Distribution

- ☒ Enable Cross-Zone Load Balancing ⓘ
- ☒ Enable Connection Draining ⓘ 300 seconds

Option D is incorrect because Route 53 Latency Based Routing resolves the DNS queries with the resources that provide the best latency. It will not help in this scenario.

To get more information on ELB cross load balancing, please refer to the link:

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

Ask our Experts



QUESTION 49

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Which of the following items are required to allow an application deployed on an EC2 instance to write data to a DynamoDB table? Assume that no security keys are allowed to be stored on the EC2 instance.

Choose 3 options from the below:

- ☐ A. Create an IAM Role that allows write access to the DynamoDB table ✓
- ☐ B. Add an IAM Role to a running EC2 instance ✓
- ☐ C. Create an IAM User that allows write access to the DynamoDB table
- ☐ D. Add an IAM User to a running EC2 instance
- ☐ E. Launch an EC2 Instance with the IAM Role included in the launch configuration ✓

Explanation :

Answer – A,B and E.

To enable an AWS service to access another one, the most important requirement is to create an appropriate IAM Role and attaching that role to the service that needs the access.

Option A is CORRECT because it create the appropriate IAM Role for accessing the DynamoDB table.

Option B is CORRECT because you can attach the role to a running EC2 instance that needs the access.

Option C and D are incorrect because IAM Role is preferred and more secured way than IAM User.

Option E is CORRECT because it launches the EC2 instance after attaching the required role.

See the steps below:

1. Create the IAM Role with appropriate permissions

Create role

1

2

3

Select type of trusted entity

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

**SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	DMS	Elastic Transcoder	Machine Learning	SageMaker
Application Auto Scaling	Data Pipeline	ElasticLoadBalancing	MediaConvert	Service Catalog
Auto Scaling	DeepLens	Glue	OpsWorks	Step Functions
Batch	Directory Service	Greengrass	RDS	Storage Gateway

* Required

Cancel

Next: Permissions

Create role

1

2

3

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Refresh

Filter: Policy type

Showing 8 results

	Policy name	Attachments	Description
<input checked="" type="checkbox"/>	AmazonDynamoDBFullAccess	1	Provides full access to Amazon DynamoDB via the AWS Ma...
<input type="checkbox"/>	AmazonDynamoDBFullAccesswithDataPipeline	0	Provides full access to Amazon DynamoDB including Export/...
<input type="checkbox"/>	AmazonDynamoDBReadOnlyAccess	0	Provides read only access to Amazon DynamoDB via the AW...
<input type="checkbox"/>	AWSApplicationAutoscalingDynamoDBTableP...	0	Policy granting permissions to Application Auto Scaling to ac...
<input type="checkbox"/>	AWSLambdaDynamoDBExecutionRole	0	Provides list and read access to DynamoDB streams and writ...
<input type="checkbox"/>	AWSLambdaInvocation-DynamoDB	0	Provides read access to DynamoDB Streams.
<input type="checkbox"/>	DynamoDBAutoscalePolicy	1	This policy will be used for the DDB Autoscaling feature. Plea...
<input type="checkbox"/>	DynamoDBReadOnlyAccessDataPolicy	0	Permissions required by DynamoDB for access to data...

* Required

Cancel

Previous

Next: Review

Create role

1 2 3

Review

Provide the required information below and review this role before you create it.

Role name*
Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies  AmazonDynamoDBFullAccess [↗](#)

* Required

[Cancel](#)

[Previous](#)

[Create role](#)

2. Launch an EC2 instance with this role

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower price access management role to the instance, and more.

Number of instances ⓘ [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ [↻](#) [Create new VPC](#)

Subnet ⓘ [Create new subnet](#)

Auto-assign Public IP ⓘ

IAM role ⓘ [↻](#) [Create new IAM role](#)

Shutdown behavior ⓘ

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring

[Additional charges apply](#)

[Cancel](#)

[Previous](#)

[Review and Launch](#)

3. Attach the role to a running EC2

Launch Instance ▼ Connect Actions ^

search : i-0c35336ce32dc75c6

Name	Instance ID	Availability Zone	Instance State	Sta
	i-0c35336ce32dc75c6			

- Connect
- Get Windows Password
- Launch More Like This
- Instance State
- Instance Settings**
 - Add/Edit Tags
 - Attach to Auto Scaling Group
 - Attach/Replace IAM Role**
 - Change Instance Type
 - Change Termination Protection
 - View/Change User Data
 - Change Shutdown Behavior
 - Change T2 Unlimited
 - Get System Log
 - Get Instance Screenshot
 - Modify Instance Placement
- Image
- Networking
- CloudWatch Monitoring

Instance: **i-0c35336ce32dc75c6** Public DNS: ec2-54-174-255-161.compute-1.amazonaws.com

Instances > Attach/Replace IAM Role

Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-0c35336ce32dc75c6 ()

IAM role* DynamoDBAccessRole



Create new IAM role



Reference Link:

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

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

<https://aws.amazon.com/about-aws/whats-new/2017/02/new-attach-an-iam-role-to-your-existing-amazon-ec2-instance/> (<https://aws.amazon.com/about-aws/whats-new/2017/02/new-attach-an-iam-role-to-your-existing-amazon-ec2-instance/>)

Ask our Experts



Your customer wishes to deploy an enterprise application on AWS which will consist of several web servers, several application servers and a small (50GB) Oracle database. The information is stored, both in the database and the file systems of the various servers. The backup system must support database recovery, whole server and whole disk restores, and individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database.

Which backup architecture will meet these requirements?

- ☐ A. Backup RDS using automated daily DB backups. Backup the EC2 instances using AMLs, and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore. ✓
- ☐ B. Backup RDS using a Multi-AZ Deployment. Backup the EC2 instances using AMLs, and supplement by copying file system data to S3 to provide file level restore.
- ☐ C. Backup RDS using automated daily DB backups. Backup the EC2 instances using EBS snapshots and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore.
- ☐ D. Backup RDS database to S3 using Oracle RMAN. Backup the EC2 instances using AMLs, and supplement with EBS snapshots for individual volume restore.

Explanation :

Answer - A

Option A is CORRECT because (a) it uses automated daily backups, from which the recovery can be made quickly, (b) the file-level backup to S3 will ensure that the recovery can be done at the individual file level - which satisfies the requirements

Option B is incorrect because Multi-AZ deployment is for Disaster Recovery, not for data backup.

Option C is incorrect because Glacier is an archival solution and most certainly will not meet the criteria of RTO of 2 hours.

Option D is incorrect because Amazon RDS does not use RMAN for backups. See the link given in the "More information" section.

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

<http://www.boyter.org/wp-content/uploads/2014/12/Backup-And-Recovery-ApproachesUsing-Aws.pdf> (<http://www.boyter.org/wp-content/uploads/2014/12/Backup-And-Recovery-ApproachesUsing-Aws.pdf>)

<https://blogs.oracle.com/pshuff/amazon-rds> (<https://blogs.oracle.com/pshuff/amazon-rds>)

Ask our Experts



QUESTION 51

UNATTEMPTED

SECURITY

How can you secure data at rest on an EBS volume?

- ☐ A. Attach the volume to an instance using EC2's SSL interface.
- ☐ B. Write the data randomly instead of sequentially.
- ☐ C. Encrypt the volume using the S3 server-side encryption service.
- ☐ D. Create an IAM policy that restricts read and write access to the volume.
- ☐ E. Use an encrypted file system on top of the EBS volume. ✓

Explanation :

Answer – E.

In order to secure data at rest on an EBS volume, you either have to encrypt the volume when it is being created or encrypt the data after the volume is created. Hence, option E is CORRECT.

For more information on EBS encryption, please refer to the link

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

(<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>)

Ask our Experts



A company needs to monitor the read and write IOPs metrics for their AWS MySQL RDS instance and send real-time alerts to their operations team. Which AWS services can accomplish this?

Choose 2 options from the below:

- ☐ A. Amazon Simple Email Service
- ☐ B. Amazon CloudWatch ✓
- ☐ C. Amazon Simple Queue Service
- ☐ D. Amazon Route 53
- ☐ E. Amazon Simple Notification Service ✓

Explanation :

Answer – B and E.

Option A is incorrect as SNS would be a better choice for sending real time notifications compared to SES.

Option B is CORRECT because CloudWatch is used for monitoring the metrics pertaining to the AWS resources.

Option C is incorrect because SQS can neither monitor any metrics, nor send out any real time notifications.

Option D is incorrect because Route 53 cannot monitor any metrics.

Option E is CORRECT because SNS is used for sending the real time notifications based on the thresholds set in CloudWatch.

For more information on cloudwatch metrics, please refer to the link:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html
(http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html)

Ask our Experts



A custom script needs to be passed to a new Amazon Linux instances created in your Auto Scaling group. Which feature allows you to accomplish this?

- ☒ A. User data ✓
- ☐ B. EC2Config service
- ☐ C. IAM roles
- ☐ D. AWS Config

Explanation :

Answer – A

When you configure an instance during creation, you can add custom scripts to the User data section.

So in Step 3 of creating an instance, in the Advanced Details section, we can enter custom scripts in the User Data section. The below script installs Perl during the instance creation of the EC2 instance.

Step 3: Configure Instance Details

Additional charges apply.

Tenancy ⓘ Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

▼ Network interfaces ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface ▼	subnet-95ed8dd1 ▼	Auto-assign	Add IP

Add Device

▼ Advanced Details

User data ⓘ ☒ As text ☐ As file ☐ Input is already base64 encoded

```
yum install perl-Switch perl-DateTime perl-Sys-Syslog perl-LWP-Protocol-https -y
```

For more information on user data please refer to the URL:

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

Ask our Experts



You have multiple Amazon EC2 instances running in a cluster across multiple Availability Zones within the same region. How will you ensure that the EC2 instances will communicate with AWS services with out any bandwidth restrictions and also perform with highest network performance, low latency and jitter?

Choose 3 options from the below:

- ☐ A. Cluster placement group
- ☐ B. Enhanced networking ✓
- ☐ C. Amazon PV AMI
- ☐ D. Amazon HVM AMI ✓
- ☐ E. Amazon Linux
- ☐ F. Amazon VPC Endpoints ✓

Explanation :

Answer - B, D, and F

Option A is Incorrect. A cluster placement group is a logical grouping of instances within a single Availability Zone and it cannot span multiple AZ's.

Option B is CORRECT because Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types.

Option C is incorrect because it is recommended to use HVM AMIs for better performance compared to PV AMIs.

option D is CORRECT because HVM AMIs take advantage of Enhanced Networking; whereas PV AMIs do not.

Option E is incorrect because using Amazon Linux does not necessarily improve any performance.

Option F is CORRECT because VPC endpoints allow communication between instances in the VPC and AWS services without imposing availability risks or bandwidth constraints on the network traffic.

For more information on Enhanced Networking, please visit the URL

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>

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

Linux Amazon Machine Images use one of two types of virtualization: paravirtual (PV) or hardware virtual machine (HVM). The main difference between PV and HVM AMIs is the way in which they boot and whether they can take advantage of special hardware extensions (CPU, network, and storage) for better performance. For the best performance, we recommend that you use current generation instance types and HVM AMIs when you launch your instances. For more information on Enhanced Networking, please visit the URL http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization_types.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/virtualization_types.html)

Ask our Experts



QUESTION 55

UNATTEMPTED

COSTING

You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out which video should be transcoded and then runs a transcoding process. If this process is interrupted, the videos will be transcoded by another instance based on the queuing system. You have a large backlog of videos which need to be transcoded and would like to reduce this backlog by adding more instances. You will need these instances only until the backlog is reduced. Which type of Amazon EC2 instances should you use to reduce the backlog in the most cost-efficient way?

- ☐ A. Reserved instances
- ☒ B. Spot instances ✓
- ☐ C. Dedicated instances
- ☐ D. On-demand instances

Explanation :

Answer – B

Since this is like a batch processing job, the best type of instance to use is a Spot instance. Since these jobs don't last for the entire duration of the year, they can bid upon and allocated and deallocated as requested.

Option A and C are incorrect because the application need the instances only until the backlog is reduced. With reserved/dedicated instances, there is a possibility that the instances might get idle after the backlog reduction. So, this is a costly solution.

Option B is CORRECT because (i) they are less expensive than reserved instances, (ii) interruption in the transcoding process is affordable since the videos will be transcoded by another instance based on the queuing system.

Option D is incorrect because (i) on-demand instances are most expensive, (ii) you can afford interruption in the transcoding process, and (iii) on demand instances would have been suited if there was no alternate way of transcoding the videos and interruption was not affordable.

For more information on Spot Instances, please visit the URL –
<https://aws.amazon.com/ec2/spot/> (<https://aws.amazon.com/ec2/spot/>)

Ask our Experts



QUESTION 56

UNATTEMPTED

SECURITY

A company has a requirement to host an application behind an AWS ELB. The application will be supporting multiple device platforms. Each device platform will need separate SSL certificates assigned to it.

Which of the below options is the best setup in AWS to fulfill the above requirement?

- ☐ A. Setup a hybrid architecture to handle multiple SSL certificates by using 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. You just need to set single ELB. Since it supports multiple SSL certificates, it should be sufficient enough for the different device platforms
- ☐ D. Create multiple ELB's for each type of certificate for each device platform.

Explanation :

Answer – B

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 A is incorrect because it is not cost effective to handle such hybrid architecture.
Option C is incorrect because even though ELB supports multiple SSL certificates, distributing the load based on the platform type will not be feasible. You will still require multiple ELBs.
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



QUESTION 57

UNATTEMPTED

SCALABILITY & ELASTICITY

You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic MapReduce job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO. You recently improved overall performance of the website using CloudFront 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 do you fix your usage dashboard?

- ☐ A. Enable CloudFront to deliver access logs to S3 and use them as input of the Elastic MapReduce job. ✓
- ☐ B. Turn on CloudTrail and use trail log tiles on S3 as input of the Elastic MapReduce job.
- ☐ C. Change your log collection process to use CloudWatch ELB metrics as input of the Elastic MapReduce job.
- ☐ D. Use Elastic Beanstalk "Rebuild Environment" option to update log delivery to the Elastic MapReduce job.
- ☐ E. Use Elastic Beanstalk "Restart App Server(s)" option to update log delivery to the Elastic MapReduce job.

Explanation :

Answer - A

Option A is CORRECT because the website is now only accessible via CloudFront. So, for the dashboard to have the up-to-date information via EMR, the logs from the CloudFront must be stored on S3 (to be analyzed by the EMR). Once these logs are delivered to S3, the dashboard should show the correct traffic information.

Option B is incorrect because CloudTrail log will not show the required information, it will only show the insights of the AWS services and APIs accessed by the application.

Option C is incorrect because the dashboard must be showing the information about the traffic pertaining to the website. CloudWatch will show the information based on the metrics related to AWS resources (not the website).

Option D is incorrect because configuration of the Elastic Beanstalk environment is independent of the CloudFormation setting. In order to have the information related to the dynamic content, the logs created by the CloudFormation must be delivered to S3. "Rebuild Environment" of Elastic Beanstalk will not be of any use.

Option E is incorrect because "Restart App Server(s)" causes the environment to restart the application container server running on each Amazon EC2 instance. It is totally unrelated to the information that is shown by the dashboard.

Ask our Experts



You decide to configure a bucket for static website hosting. As per the AWS documentation, you create a bucket named 'mybucket.com' and then you enable website hosting with an index document of 'index.html' and you leave the error document as blank. You then upload a file named 'index.html' to the bucket. After clicking on the endpoint of mybucket.com.s3-website-us-east-1.amazonaws.com you receive 403 Forbidden error. You then change the CORS configuration on the bucket so that everyone has access, however, you still receive the 403 Forbidden error. What additional step do you need to do so that the endpoint is accessible to everyone?

Choose the correct option from the below:

- ☐ A. Register mybucket.com on Route53
- ☐ B. Wait for the DNS change to propagate
- ☐ C. You need to add a name for the error document, because it is a required field
- ☒ D. Change the permissions on the index.html file also, so that everyone has access ✓

Explanation :

Answer – D

You are receiving the 403 Forbidden Error because you do not have the permissions to view the index.html file.

Option A is incorrect because this is an S3 hosted website, Route 53 does not come into picture.

Option B is incorrect because it is a static website hosted on S3. This issue is not related to DNS resolution.

Option C is incorrect because even if you add the error document, you will get the error, because you need to set the proper permissions.

Option D is CORRECT because it sets the appropriate permissions so that the user has access to the index.html.

For more information on web site hosting in S3, please visit the below link:

- <http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>)

Note:

The question is referring to Configuring a bucket for Website Hosting. In this scenario Route53 is not required. However extra configuration in S3 is needed other than making it public.

For more information please refer:

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/IndexDocumentSupport.html>
(<https://docs.aws.amazon.com/AmazonS3/latest/dev/IndexDocumentSupport.html>)

Ask our Experts



QUESTION 59

UNATTEMPTED

SECURITY

Server-side encryption is about data encryption at rest. That is, Amazon S3 encrypts your data at the object level as it writes it to disk in its data centers and decrypts it for you when you go to access it. There are a few different options depending on how you choose to manage the encryption keys. One of the options is called 'Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)'. Which of the following best describes how this encryption method works?

Choose the correct option from the below:

- ☐ A. There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3 and also provides you with an audit trail of when your key was used and by whom.
- ☐ B. Each object is encrypted with a unique key employing strong encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. ✓
- ☐ C. You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disk, and decryption, when you access your objects.
- ☐ D. A randomly generated data encryption key is returned from Amazon S3, which is used by the client to encrypt the object data.

Explanation :

Answer – B

Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Option A is incorrect because there are no separate permissions to the key that protects the data key.

Option B is CORRECT because as mentioned above, each object is encrypted with a strong unique key and that key itself is encrypted by a master key.

Option C is incorrect because the keys are managed by the AWS.

Option D is incorrect because there is no randomly generated key and client does not do the encryption.

For more information on S3 encryption, please visit the link

<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html>)

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html>

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

Ask our Experts



QUESTION 60

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Explain what the following resource in a CloudFormation template does.

Choose the best possible answer.

```
"SNSTopic" : {  
  "Type" : "AWS::SNS::Topic",  
  "Properties" : {  
    "Subscription" : [{  
      "Protocol" : "sqs",
```

```
"Endpoint": { "Fn::GetAtt": [ "SQSQueue", "Arn" ] }  
}  
}
```

- ☐ A. Creates an SNS topic which allows SQS subscription endpoints to be added as a parameter on the template
- ☐ B. Creates an SNS topic and adds a subscription ARN endpoint for the SQS resource named Arn
- ☐ C. Creates an SNS topic and then invokes the call to create an SQS queue with a logical resource name of SQSQueue
- ☐ D. Creates an SNS topic and adds a subscription ARN endpoint for the SQS resource created under the logical name SQSQueue ✓

Explanation :

Answer – D

Option A is incorrect because it is not adding any parameter in the template.

Option B is incorrect because it is not adding a subscription endpoint for the SQS resource named Arn. It is actually creating an SNS topic and adding a subscription ARN endpoint for the SQS resource name SQSQueue.

Option C is incorrect because it does not create any SQS queue.

Option D is CORRECT because it creates an SNS topic and adds a subscription ARN endpoint for the SQS resource.

For more information on Fn:: GetAtt function please refer to the below link

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-getatt.html>

(<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-getatt.html>)

Ask our Experts



A customer implemented AWS Storage Gateway with a gateway-cached volume at their main office. An event takes the link between the main and branch office offline. Which methods will enable the branch office to access their data?

Choose 3 answers:

- ☐ A. Use a HTTPS GET to the Amazon S3 bucket where the files are located.
- ☐ B. Restore by implementing a lifecycle policy on the Amazon S3 bucket.
- ☐ C. Make an Amazon Glacier Restore API call to load the files into another Amazon S3 bucket within four to six hours.
- ☐ D. Launch a new AWS Storage Gateway instance AMI in Amazon EC2, and restore from a gateway snapshot. ✓
- ☐ E. Create an Amazon EBS volume from a gateway snapshot, and mount it to an Amazon EC2 instance. ✓
- ☐ F. Launch an AWS Storage Gateway virtual iSCSI device at the branch office, and restore from a gateway snapshot. ✓

Explanation :

Answers - D, E, & F

Option A is incorrect because, all gateway-cached volume data and snapshot data is stored in Amazon S3 encrypted at rest using server-side encryption (SSE) and it cannot be visible or accessed with S3 API or any other tools. (Ref: <https://forums.aws.amazon.com/thread.jspa?threadID=109748>)

Option B is incorrect you cannot apply Lifecycle Policies as the AWS Storage Gateway does not give you that option.

Option C is incorrect because the cached volumes are never stored to Glacier.

Option D is CORRECT because, you can take point-in-time snapshots of gateway volumes that are made available in the form of Amazon EBS snapshots. You can launch an EC2 instance from that.

Option E is CORRECT because, you can take point-in-time snapshots of gateway volumes that are made available in the form of Amazon EBS snapshots. A new EBS volume can be created from the snapshot which can be mounted to an existing EC2 instance.

Option F is CORRECT because, you can take point-in-time snapshots of gateway volumes that are made available in the form of Amazon EBS snapshots. A Volume Gateway allows you to mount iSCSI devices that you can mount to on-premise machines. You can then restore the data from the point-in-time snapshot.

For more information on this topic, please refer to the AWS FAQs:

<https://aws.amazon.com/storagegateway/faqs/>
(<https://aws.amazon.com/storagegateway/faqs/>)
(<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-anatomy.html>)

Ask our Experts



QUESTION 62

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You created three S3 buckets – “mydomain.com”, “downloads.mydomain.com”, and “www.mydomain.com”. You uploaded your files, enabled static website hosting, specified both of the default documents under the “enable static website hosting” header, and set the “Make Public” permission for the objects in each of the three buckets. All that’s left for you to do is to create the Route 53 Aliases for the three buckets. You are going to have your end users test your websites by browsing to <http://mydomain.com/error.html>, <http://downloads.mydomain.com/index.html>, and <http://www.mydomain.com>. What problems will your testers encounter?

Choose an option from the below:

- ☐ A. <http://mydomain.com/error.html> will not work because you did not set a value for the error.html file
- ☐ B. <http://www.mydomain.com> will not work because the URL does not include a file name at the end of it
- ☐ C. There will be no problems, all three sites should work ✓
- ☐ D. <http://downloads.mydomain.com/index.html> will not work because the “downloads” prefix is not a supported prefix for S3 websites using Route 53 aliases

Explanation :

Answer – C

Previously only allowed domain prefix when we are creating AWS Route53 aliases for AWS S3 static websites was the “www”.

However, this is no longer the case. You can now use other sub-domains.

For more information on S3 web site hosting please visit the below link:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

(<http://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>)

Ask our Experts



QUESTION 63

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Your supervisor is upset about the fact that SNS topics that he subscribed to are now cluttering up his email inbox. How can he stop receiving the email from SNS without disrupting other users' ability to receive the email from SNS?

Choose 2 options from the below:

- ☐ A. You can delete the subscription from the SNS topic responsible for the emails ✓
- ☐ B. You can delete the endpoint from the SNS subscription responsible for the emails
- ☐ C. You can delete the SNS topic responsible for the emails
- ☐ D. He can use the unsubscribe information provided in the emails ✓

Explanation :

Answer – A and D

Every request has a unsubscribe URL which can be used. Also from the aws console , one can just delete the subscription

Option A is CORRECT because deleting the subscription for the user from the SNS topic will

ensure that he will not receive any notifications (basically just unsubscribe him).
Option B is incorrect because you cannot delete the endpoint from the SNS subscription.
Option C is incorrect because if you delete the topic then none of the subscribers will get any notifications.
Option D is CORRECT because the notifications has an option to unsubscribe which the user can avail to stop receiving the notifications.

For more information on SNS subscription please visit the below link
http://docs.aws.amazon.com/sns/latest/api/API_Subscribe.html
(http://docs.aws.amazon.com/sns/latest/api/API_Subscribe.html)

Ask our Experts



QUESTION 64

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have created an Elastic Load Balancer with Duration-Based sticky sessions enabled in front of your six EC2 web application instances in US-West-2. For High Availability, there are three web application instances in Availability Zone 1 and three web application instances in Availability Zone 2. To load test, you set up a software-based load tester in Availability Zone 2 to send traffic to the Elastic Load Balancer, as well as letting several hundred users browse to the ELB's hostname.

After a while, you notice that the users' sessions are spread evenly across the EC2 instances in both AZ's, but the software-based load tester's traffic is hitting only the instances in Availability Zone 2. What steps can you take to resolve this problem?

Choose 2 correct options from the below:

- ☐ A. Create a software-based load tester in US-East-1 and test from there.
- ☐ B. Force the software-based load tester to re-resolve DNS before every request. ✓
- ☐ C. Use a third party load-testing service to send requests from globally distributed clients. ✓

☐ **D. Switch to application-controlled sticky sessions.**

Explanation :

Answer – B and C

When you create an elastic load balancer, a default level of capacity is allocated and configured. As Elastic Load Balancing sees changes in the traffic profile, it will scale up or down. The time required for Elastic Load Balancing to scale can range from 1 to 7 minutes, depending on the changes in the traffic profile. When Elastic Load Balancing scales, it updates the DNS record with the new list of IP addresses. To ensure that clients are taking advantage of the increased capacity, Elastic Load Balancing uses a TTL setting on the DNS record of 60 seconds. It is critical that you factor this changing DNS record into your tests. If you do not ensure that DNS is re-resolved or use multiple test clients to simulate increased load, the test may continue to hit a single IP address when Elastic Load Balancing has actually allocated many more IP addresses. Because your end users will not all be resolving to that single IP address, your test will not be a realistic sampling of real-world behavior.

Option A is incorrect because creating load tester in US-East-1 will face the same problem of traffic hitting only the instances in that AZ.

Option B is CORRECT because if you do not ensure that DNS is re-resolved the test may continue to hit the single IP address.

Option C is CORRECT because if the requests come from globally distributed users, the DNS will not be resolved to a single IP address and the traffic would be distributed evenly across multiple instances.

Option D is incorrect because the traffic will be routed to the same back-end instances as the users continue to access your application. The load will not be evenly distributed across the AZs.

Please refer to the below article for more information:

<http://aws.amazon.com/articles/1636185810492479>

(<http://aws.amazon.com/articles/1636185810492479>)

Ask our Experts



You run an ad-supported photo sharing website using S3 to serve photos to visitors of your site. At some point you find out that other sites have been linking to the photos on your site, causing loss to your business. What is a cost-effective method to mitigate this?

Choose the correct answer from the below options:

- ☐ A. Use CloudFront distributions for static content.
- ☐ B. Store photos on an EBS volume of the web server.
- ☐ C. Remove public read access and use signed URLs with expiry dates. ✓
- ☐ D. Block the IPs of the offending websites in Security Groups.

Explanation :

Answer – C

You can distribute private content using a signed URL that is valid for only a short time—possibly for as little as a few minutes. Signed URLs that are valid for such a short period are good for distributing content on-the-fly to a user for a limited purpose, such as distributing movie rentals or music downloads to customers on demand.

Option A is incorrect because using CloudFront is an expensive option compared to using signed URLs.

Option B is incorrect because the website is hosted on S3.

Option C is CORRECT because, as mentioned above, it will ensure that only the trusted/authenticated users get access to the content.

Option D is incorrect because the website is hosted on S3 which does not have any security group setting.

For more information on Signed URL's please visit the below link

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>)

Ask our Experts



You are using DynamoDB to store data in your application. One of the tables named "Users", you have defined "UserID" as its primary key. However, you envision that, in some cases, you might need to query the table by "UserName" which cannot be set as primary key. What changes would you do to this table to be able to query using UserName?

Choose correct option from the below:

- ☐ A. Create a second table that contains all the information, but make UserName the primary key.
- ☐ B. Create a hash and range primary key.
- ☒ C. Create a secondary index. ✓
- ☐ D. Partition the table using UserName rather than UserID.

Explanation :

Answer – C

Amazon DynamoDB provides fast access to items in a table by specifying primary key values. However, many applications might benefit from having one or more secondary (or alternate) keys available, to allow efficient access to data with attributes other than the primary key. To address this, you can create one or more secondary indexes on a table, and issue Query or Scan requests against these indexes.

Option A is incorrect because creating another table is costly and unnecessary.

Option B is incorrect because UserName cannot be primary key.

Option C is CORRECT because, as mentioned above, creating a secondary index on UserName would allow the user to efficiently access the table via querying on this attribute rather than UserID which is the primary key.

Option D is incorrect because DynamoDB tables are partitioned based on the primary key and you cannot make UserName as the primary key.

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



QUESTION 67

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

A web application is currently hosted on an on-premise location. There is an ad-campaign underway and there is a probability that the influx of traffic on the website is going to increase. The company does not have the time to migrate this application to AWS.

Which scenario below will provide full site functionality, while helping to improve the ability of your application to take the influx of traffic 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 because this is the only option. 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.
- ☐ 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 because ELB cannot do balancing between AWS EC2 instances and on-premise instances.

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

DEPLOYMENT MANAGEMENT

Which section in your CloudFormation template would you modify to fire up different instance sizes based off of environment type (Dev/Staging/Production)?

Choose the correct answer from below options:

- ☐ A. Outputs
- ☐ B. Resources
- ☐ C. Mappings
- ☒ D. Conditions ✓

Explanation :

Answer – D

The optional Conditions section includes statements that define when a resource is created or when a property is defined. For example, you can compare whether a value is equal to another value. Based on the result of that condition, you can conditionally create resources. If you have multiple conditions, separate them with commas.

For more information on Cloudformation conditions please visit the below link

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html>

(<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html>)

Note:

As per AWS documentation,

You might use conditions when you want to reuse a template that can create resources in different contexts, such as a test environment versus a production environment. In your template, you can add an ***EnvironmentType*** input parameter, which accepts either ***prod*** or ***test*** as inputs. For the production environment, you might include Amazon EC2 instances with certain capabilities; however, for the test environment, you want to use reduced capabilities to save money. **With conditions, you can define which resources are created and how they're configured for each environment type.**

Conditions are evaluated based on input parameter values that you specify when you create or update a stack. Within each condition, you can reference another condition, a parameter value, or a mapping. After you define all your conditions, you can associate them with resources and resource properties in the ***Resources*** and ***outputs*** sections of a template.

For more details, please check the below AWS Docs:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html>

(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-section-structure.html>)

Ask our Experts



QUESTION 69

UNATTEMPTED

SECURITY

There are currently multiple applications hosted in a VPC. During monitoring, it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Addresses?

- ☐ A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.
- ☐ B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block. ✓
- ☐ C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.
- ☐ D. Modify the Windows Firewall settings on all AMI's that your organization uses in that VPC to deny access from the IP address block.

Explanation :

Answer – B

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

Option A and D are incorrect because (a) it will only work for windows-based instances, and (b) better approach is to block the traffic at the subnet layer via NACL rather than instance layer (windows firewall).

Option B is CORRECT because the best way to allow or deny IP address-based access to the resources in the VPC is to configure rules in the Network access control list (NACL) which are applied at the subnet level.

Option C is incorrect because (a) you cannot explicitly deny access to particular IP addresses via security group, and (b) better approach is to block the traffic at the subnet layer via NACL rather than instance layer (security group).

For more information on network ACL's please refer to the below link:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLS.html

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

Ask our Experts



QUESTION 70

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have an Auto Scaling group associated with an Elastic Load Balancer (ELB). You have noticed that instances launched via the Auto Scaling group are being marked unhealthy due to an ELB health check but these unhealthy instances are not being terminated. What do you need to do to ensure that the instances marked unhealthy by the ELB will be terminated and replaced?

- ☐ A. Change the thresholds set on the Auto Scaling group health check
- ☐ B. Add an Elastic Load Balancing health check to your Auto Scaling group ✓
- ☐ C. Increase the value for the Health check interval set on the Elastic Load Balancer
- ☐ D. Change the health check set on the Elastic Load Balancer to use TCP rather than HTTP checks

Explanation :

Answer – B

To discover the availability of your EC2 instances, an ELB periodically sends pings, attempts connections, or sends requests to test the EC2 instances. These tests are called health checks. The status of the instances that are healthy at the time of the health check is InService. The status of any instances that are unhealthy at the time of the health check is OutOfService.

When you allow the Auto Scaling group (ASG) to receive the traffic from the ELB, it gets notified when the instance becomes unhealthy and then it terminates it. See the images in the "More information..." section for more details.

Option A is incorrect because changing the threshold will not enable ASG to know about the unhealthy instances.

Option B is CORRECT because when you associate the ELB with ASG, you allow the ASG to receive the traffic from that ELB. As a result, the ASG will get aware about the unhealthy instances and it terminates them.

Option C is incorrect because increasing the interval will still not communicate the information about the unhealthy instances to the ASG.

Option D is incorrect because this setting will not communicate the information about the unhealthy instances to the ASG either.

More information on ELB with Auto Scaling Group:

1. Configure Auto Scaling group details

2. Configure scaling policies

3. Configure Notifications

4. Configure Tags

5. Review

Create Auto Scaling Group

Launch Configuration ⓘ

LC1

Group name ⓘ

Group1

Group size ⓘ

Start with 1 instances

Network ⓘ

vpc-cdc05eab (172.31.0.0/16) (default)

Create new VPC

Subnet ⓘ

Create new subnet

Each instance in this Auto Scaling group will be assigned a public IP address. ⓘ

▼ Advanced Details

Load Balancing ⓘ

☒ Receive traffic from one or more load balancers

Learn about Elastic Load Balancing

Classic Load Balancers ⓘ

MyELB ✕

Target Groups ⓘ

Health Check Type ⓘ

☒ ELB ☐ EC2

Health Check Grace Period ⓘ

300 seconds

Monitoring ⓘ

Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration LC1. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency.
[Learn more](#)

Instance Protection ⓘ

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol	<input type="text" value="HTTP"/>
Ping Port	<input type="text" value="80"/>
Ping Path	<input type="text" value="/index.html"/>

Advanced Details

Response Timeout ⓘ	<input type="text" value="5"/>	seconds
Interval ⓘ	<input type="text" value="30"/>	seconds
Unhealthy threshold ⓘ	<input type="text" value="2"/>	
Healthy threshold ⓘ	<input type="text" value="10"/>	

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

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

(<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>)

Ask our Experts



QUESTION 71

UNATTEMPTED

NETWORK DESIGN

You have two Elastic Compute Cloud (EC2) instances inside a Virtual Private Cloud (VPC) in the same Availability Zone (AZ) but in different subnets. One instance is running a database and the other instance an application that will interface with the database.

You want to confirm that they can talk to each other for your application to work properly. Which two things do we need to confirm in the VPC settings so that these EC2 instances can communicate inside the VPC?

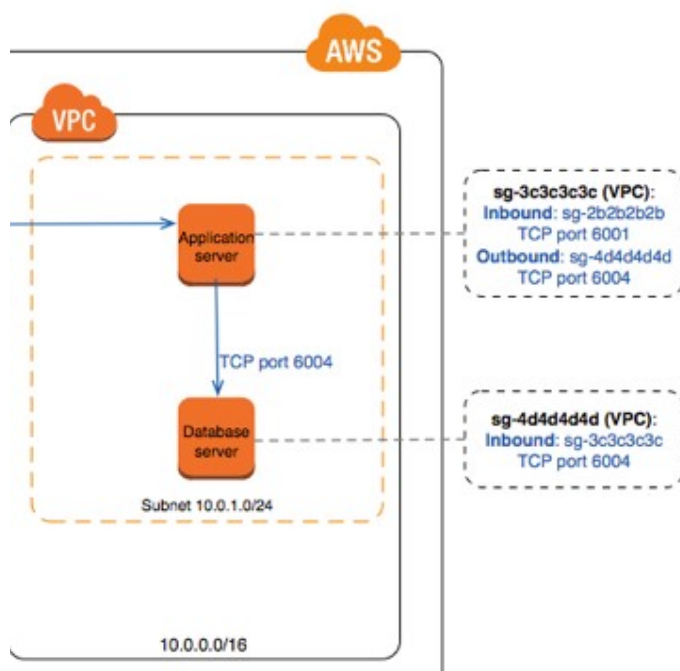
Choose 2 correct options from the below:

- ☐ A. Security groups are set to allow the application host to talk to the database on the right port/protocol. ✓
- ☐ B. Both instances are the same instance class and using the same key-pair.
- ☐ C. That the default route is set to a NAT instance or internet Gateway (IGW) for them to communicate.
- ☐ D. A network ACL that allows communication between the two subnets. ✓

Explanation :

Answer - A and D

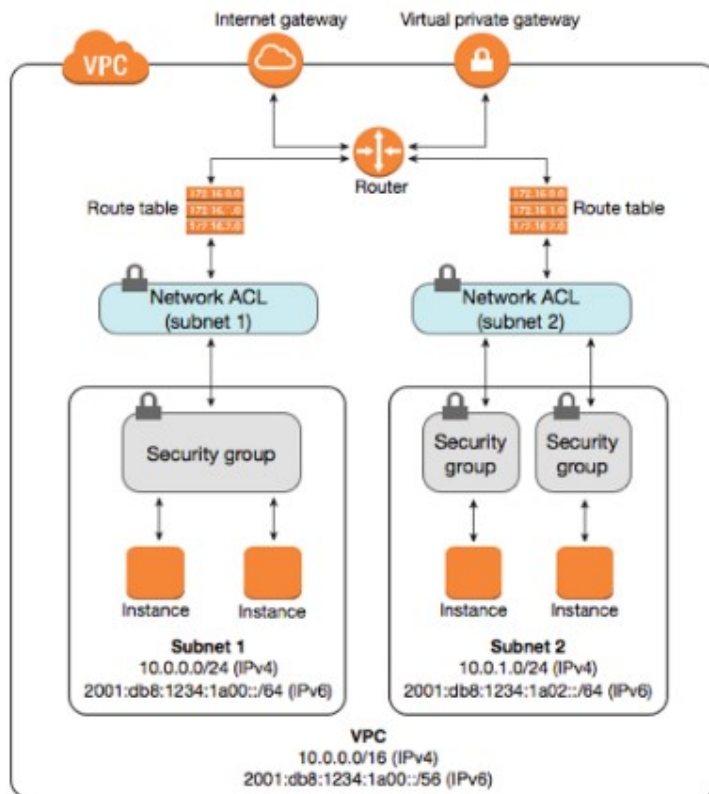
In order to have the instances communicate with each other, you need to properly configure both Security Group and Network access control lists (NACLs). For the exam, remember that Security Group operates at the instance level; where as, the NACL operates at subnet level. Option A is CORRECT because the security groups must be defined in order to allow web server to communicate with the database server. An example image from the AWS documentation is given below:



Option B is incorrect because it is not necessary to have the two instances of the same type or be using same key-pair.

Option C is incorrect because configuring NAT instance or NAT gateway will not enable the two servers to communicate with each other. NAT instance/NAT gateway are used to enable the communication between instances in the private subnets and internet.

Option D is CORRECT because the two servers are in two separate subnets. In order for them to communicate with each other, you need to have the NACL's configured as shown below:



For more information on VPC and Subnets, please visit the below URL:

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



You are managing a legacy application inside VPC with hard-coded IP addresses in its configuration. Which mechanisms will allow the application to failover to new instances without the need for reconfiguration?

Choose 2 options from the below:

- ☐ A. Create an ELB to reroute traffic to the failover instance
- ☒ B. Create a secondary ENI that can be moved to the failover instance ✓
- ☐ C. Use Route53 health checks to reroute the traffic to the failover instance
- ☒ D. Assign a secondary private IP address to the primary ENI of the failover instance ✓

Explanation :

Answer - B and D

Option A is incorrect because rerouting to a failover instance in case of hardcoded IP address is not possible via ELB.

Option B is CORRECT because the attributes of a network interface follow it as it's attached or detached from an instance and reattached to another instance. When you move a network interface from one instance to another, network traffic is redirected to the new instance.

Option C is incorrect because Route 53 cannot reroute the traffic between the to failover instance with the same IP address.

Option D is CORRECT because you can have a secondary IP address that can be configured on the primary ENI of the failover instance.

Best Practices for Configuring Network Interfaces

- You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).
- You can detach secondary (ethN) network interfaces when the instance is running or stopped. However, you can't detach the primary (eth0) interface.
- You can attach a network interface in one subnet to an instance in another subnet in the same VPC; however, both the network interface and the instance must reside in the same Availability Zone.
- When launching an instance from the CLI or API, you can specify the network interfaces to attach to the instance for both the primary (eth0) and additional network interfaces.

- Launching an Amazon Linux or Windows Server instance with multiple network interfaces automatically configures interfaces, private IPv4 addresses, and route tables on the operating system of the instance.
- A warm or hot attach of an additional network interface may require you to manually bring up the second interface, configure the private IPv4 address, and modify the route table accordingly. Instances running Amazon Linux or Windows Server automatically recognize the warm or hot attach and configure themselves.
- Attaching another network interface to an instance (for example, a NIC teaming configuration) cannot be used as a method to increase or double the network bandwidth to or from the dual-homed instance.
- If you attach two or more network interfaces from the same subnet to an instance, you may encounter networking issues such as asymmetric routing. If possible, use a secondary private IPv4 address on the primary network interface instead. For more information, see [Assigning a Secondary Private IPv4 Address](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP) (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP>).

For more information on Network Interfaces, please visit the below URL:

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

Ask our Experts



QUESTION 73

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

A media company produces new video files on-premises every day with a total size of around 100GB after compression. All files have a size of 1 -2 GB and need to be uploaded to Amazon S3 every night in a fixed time window between 3 AM and 5 AM. Current upload takes almost 3 hours, although less than half of the available bandwidth is used. What step(s) would ensure that the file uploads are able to complete in the allotted time window?

- ☐ A. Increase your network bandwidth to provide faster throughput to S3
- ☐ B. Upload the files in parallel to S3 ✓
- ☐ C. Pack all files into a single archive, upload it to S3, and then extract the files in AWS
- ☐ D. Use AWS Import/Export to transfer the video files

Explanation :

Answer – B

When uploading large videos it's always better to make use of AWS multipart file upload, especially when the bandwidth is not fully utilized.

Option A is incorrect because existing bandwidth itself is not fully utilized. Increasing the bandwidth is not going to help; in fact, it will add to the cost.

Option B is CORRECT because parallel upload of the files via AWS multipart upload will fully utilize the available bandwidth and increase the throughput. It also has additional benefits as mentioned below in the "More Information" section.

Option C is incorrect because there is a restriction on the size of upload in a single PUT operation. You cannot upload a file of size more than 5GB in a single upload. So this option is not going to help at all. You need to use multipart upload.

Option D is incorrect because this option requires you to put all the files daily on a storage drive and send it to AWS. Since the data has to be uploaded in a certain time frame and there is sufficient bandwidth already available, multipart upload is the best option compared to AWS Import/Export.

More information on and benefits of Multipart upload on S3

Below is the advantage of multipart upload:

- Improved throughput—you can upload parts in parallel to improve throughput.
- Quick recovery from any network issues—smaller part size minimizes the impact of restarting a failed upload due to a network error.
- Pause and resume object uploads—you can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload.
- Begin a upload before you know the final object size—you can upload an object as you are creating it.

For more information on Multi-part file upload for S3, please visit the URL -

<http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html>
(<http://docs.aws.amazon.com/AmazonS3/latest/dev/qfacts.html>)

Ask our Experts



QUESTION 74

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Your team is excited about the use of AWS because now they have access to "programmable Infrastructure". You have been asked to manage your AWS infrastructure in a manner similar to the way you might manage application code. You want to be able to deploy exact copies of different versions of your infrastructure, stage changes into different environments, revert back to previous versions, and identify what versions are running at any particular time (development, test, QA , and production). Which approach addresses this requirement?

- ☐ A. Use cost allocation reports and AWS Opsworks to deploy and manage your infrastructure.
- ☐ B. Use AWS CloudWatch metrics and alerts along with resource tagging to deploy and manage your infrastructure.
- ☐ C. Use AWS Beanstalk and a version control system like GIT to deploy and manage your infrastructure.
- ☐ D. Use AWS CloudFormation and a version control system like GIT to deploy and manage your infrastructure. ✓

Explanation :

Answer – D

You can use AWS Cloud Formation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You don't need to figure out the order for provisioning AWS services or the subtleties of making those dependencies work. CloudFormation takes care of this for you. After the AWS resources are deployed, you can modify and update them in a controlled and predictable way, in effect applying version control to your AWS infrastructure the same way you do with your software. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer.

Option A is incorrect because Cost Allocation Reports is not helpful for the purpose of the question.

Option B is incorrect because CloudWatch is used for monitoring the metrics pertaining to different AWS resources.

Option C is incorrect because it does not have the concept of programmable Infrastructure.

Option D is CORRECT because AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

For more information on CloudFormation, please visit the link:

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

Ask our Experts



QUESTION 75

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

What would happen to an RDS (Relational Database Service) multi-Availability Zone deployment if the primary DB instance fails?

- ☐ A. The IP address of the primary DB instance is switched to the standby DB instance.
- ☐ B. The primary RDS (Relational Database Service) DB instance reboots and remains as primary.
- ☐ C. A new DB instance is created in the standby availability zone.
- ☐ D. The canonical name record (CNAME) is changed from primary to standby.



Explanation :

Answer – D

Option A is incorrect because IP address of the primary and standby instances remain same and are not changed.

Option B is incorrect because the CNAME record of the primary DB instance changes to the standby instance.

Option C is incorrect because there is no new instance created in the standby AZ.

Option D is CORRECT because the CNAME of the primary DB instance changes to the standby instance so that there is no impact of on the application setting or any reference to the primary instance.

More information on Amazon RDS Multi-AZ deployment:

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure (for example, instance hardware failure, storage failure, or network disruption), Amazon RDS performs an automatic failover to the standby, so that you can resume database operations as soon as the failover is complete.

And as per the AWS documentation, the CNAME is changed to the standby DB when the primary one fails.

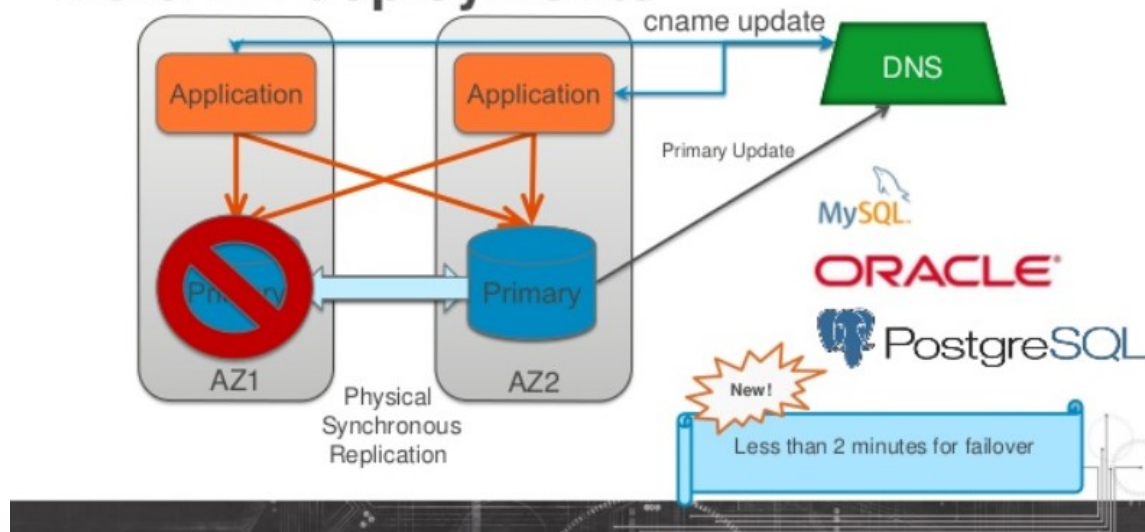
Q: What happens during Multi-AZ failover and how long does it take?

Failover is automatically handled by Amazon RDS so that you can resume database operations as quickly as possible without administrative intervention. When failing over, Amazon RDS simply flips the canonical name record (CNAME) for your DB instance to point at the standby, which is in turn promoted to become the new primary. We encourage you to follow best practices and implement database connection retry at the application layer.

Failovers, as defined by the interval between the detection of the failure on the primary and the resumption of transactions on the standby, typically complete within one to two minutes. Failover time can also be affected by whether large uncommitted transactions must be recovered; the use of adequately large instance types is recommended with Multi-AZ for best results. AWS also recommends the use of Provisioned IOPS with Multi-AZ instances, for fast, predictable, and consistent throughput performance.

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

Multi-AZ deployments



For more information on Multi-AZ RDS, please visit the link:
<https://aws.amazon.com/rds/details/multi-az/> (<https://aws.amazon.com/rds/details/multi-az/>)

Ask our Experts



QUESTION 76

UNATTEMPTED

COSTING

A user is trying to save some cost on the AWS services. Which of the below-mentioned options will not help him to save cost?

- ☐ A. Delete the unutilized EBS volumes once the instance is terminated.
- ☐ B. Delete the AutoScaling launch configuration after the instances are terminated. ✓
- ☐ C. Release the elastic IP if not required once the instance is terminated.
- ☐ D. Delete the AWS ELB after all the instances behind it are terminated.

Explanation :

Answer – B

Option A is incorrect because EBS volumes do have a costing aspect and hence deleting the unutilized volumes will save some cost.

Option B is CORRECT because an unused AutoScaling launch configuration will not cost anything.

Option C is incorrect because non-associated Elastic IP will cost you if not released.

Option D is incorrect because an ELB without any instances behind it incurs costs.

For more information on AWS Pricing, please visit the link:
<https://aws.amazon.com/pricing/services/> (<https://aws.amazon.com/pricing/services/>)

Ask our Experts



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

- ☒ A. AWS Elastic Beanstalk ✓
- ☐ B. AWS Cloudfront
- ☐ C. AWS Cloudformation
- ☐ D. AWS DevOps

Explanation :

Answer – A

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

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

Hence, A is the CORRECT answer.

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

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

We can do it on AWS CloudFormation as well in a harder way and it will be less Native:

- <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html>
(<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html>)

Ask our Experts



Your company has a lot of GPU intensive workloads. Also, these workloads are part of a process in which some steps need manual intervention. Which of the below options works out for the above-mentioned requirement?

- ☐ A. Use AWS Data Pipeline to manage the workflow. Use an auto-scaling group of G2 instances in a placement group.
- ☐ B. Use Amazon Simple Workflow (SWF) to manage the workflow. Use an autoscaling group of G2 instances in a placement group. ✓
- ☐ C. Use Amazon Simple Workflow (SWF) to manage the workflow. Use an autoscaling group of C3 instances with SR-IOV (Single Root I/O Virtualization).
- ☐ D. Use AWS data Pipeline to manage the workflow. 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 G2 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 G2 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 G2 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 G2 instances.

More information on G2 instances:

Using G2 instances is preferred. Hence option C and D are wrong.

G2

G2 instances are optimized for graphics-intensive applications.

Features:

- High Frequency Intel Xeon E5-2670 (Sandy Bridge) Processors
- High-performance NVIDIA GPUs, each with 1,536 CUDA cores and 4GB of video memory
- Each GPU features an on-board hardware video encoder designed to support up to eight real-time HD video streams (720p@30fps) or up to four real-time full HD video streams (1080p@30fps)
- Support for low-latency frame capture and encoding for either the full operating system or select render targets, enabling high-quality interactive streaming experiences

Model	GPUs	vCPU	Mem (GiB)	SSD Storage (GB)
g2.2xlarge	1	8	15	1 x 60
g2.8xlarge	4	32	60	2 x 120

Use Cases

3D application streaming, video encoding, and other server-side graphics workloads.

For more information on Instances 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



QUESTION 79

UNATTEMPTED

COSTING

An organization is generating digital policy files which are required by the admins for verification. Once the files are verified they may not be required in the future unless there is some compliance issue. Which is the best possible solution if the organization wants to save them in a cost-effective way?

- ☐ A. AWS RRS
- ☐ B. AWS S3
- ☐ C. AWS RDS
- ☐ D. AWS Glacier ✓

Explanation :

Answer – D

This question is basically asking you to choose a cost-effective archival solution. Amazon Glacier is most suited for such scenarios.

Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for data backup and archival. With Amazon Glacier, customers can reliably store their data for as little as \$0.004 per gigabyte per month. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so that they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and repair, or time-consuming hardware migrations.

Option A and B are incorrect because they are used for real time storage.

Option C is incorrect because this is a database service not an archival one.

Option D is, as mentioned above, CORRECT.

For more information on Glacier please visit the link –

<https://aws.amazon.com/glacier/details/> (<https://aws.amazon.com/glacier/details/>)

Ask our Experts



QUESTION 80

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You have large EC2 instances in your AWS infrastructure which you have recently setup. These instances carry out the task of creating JPEG files and store them on a S3 bucket and occasionally need to perform high computational tasks. After close monitoring you see that the CPUs of these instances remain idle most of the time.

Which of the below solutions will ensure better utilization of resources?

- ☐ A. Use Amazon glacier instead of S3.
- ☐ B. Add additional large instances by introducing a task group.
- ☐ C. Use T2 instances if possible. ✓
- ☐ D. Ensure the application hosted on the EC2 instances uses larger files on S3 to handle more load.

Explanation :

Answer – C

In this scenario the problem is that the large EC2 instances are mostly remaining unused. Hence, the solution should be to use instances that can cost less but still be able to carry out occasional high computational tasks.

T2 instances are Burstable Performance Instances that provide a baseline level of CPU performance with the ability to burst above the baseline. The baseline performance and ability to burst are governed by CPU Credits. T2 instances accumulate CPU Credits when they are idle, and consume CPU Credits when they are active. T2 instances are the lowest-cost Amazon EC2 instance option designed to dramatically reduce costs for applications that benefit from the ability to burst to full core performance whenever required.

Option A is incorrect because there is no issue with the current use of S3.

Option B is incorrect because adding another large instance is, on the contrary, an expensive solution and would add to the existing cost.

Option C is CORRECT because T2 instances are cost-effective and also provide a baseline level of CPU performance with the ability to burst above the baseline whenever required.

Option D is incorrect because this option is not going to make efficient use of the current instances. It will not lower the cost of the architecture.

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

<https://aws.amazon.com/ec2/instance-types/t2/> (<https://aws.amazon.com/ec2/instance-types/t2/>)

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csdp-practice-tests/quiz/13605>)

Certification

- ➔ Cloud Certification (<https://www.whizlabs.com/cloud-certification-training-courses/>)

Company

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

- ➔ 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

- ➔ 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>)