

Flat 15% OFF | Sitewide | Use Coupon - WHIZOFFER15 (<https://www.whizlabs.com/>)



[Home](https://www.whizlabs.com/learn/) (<https://www.whizlabs.com/learn/>) > [My Courses](https://www.whizlabs.com/learn/my-courses) (<https://www.whizlabs.com/learn/my-courses>)

> [AWS Certified Solutions Architect Professional](https://www.whizlabs.com/learn/course/aws-csap-practice-tests#section-1) (<https://www.whizlabs.com/learn/course/aws-csap-practice-tests#section-1>)

> [Practice Test IV](https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13607) (<https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13607>) > **Report**

PRACTICE TEST IV

Attempt 1

Marks Obtained 0 / 80

Your score is 0.0%

Completed on Tuesday , 29 January 2019 , 01:54 PM

Time Taken 00 H 00 M 42 S

Result Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Scalability & Elasticity	10	0	1	9
2	Deployment Management	19	0	0	19
3	Security	13	0	0	13
4	Data Storage	7	0	0	7
5	Network Design	12	0	0	12
6	Costing	6	0	0	6
7	Cloud Migration & Hybrid Architecture	3	0	0	3
8	High Availability and Business Continuity	10	0	0	10

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

Show Answers

All



QUESTION 1

INCORRECT

SCALABILITY & ELASTICITY

As a solution architect professional, you have been requested to launch 20 Large EC2 instances which will all be used to process huge amounts of data. There is also a requirement that these instances will need to transfer data back and forth among each other. Which of the following would be the most efficient setup to achieve this?

Choose the correct option from the below:

- ☒ A. Ensure that all the instances are placed in the same region. ✕
- ☐ B. Ensure that all instances are placed in the same availability zone.
- ☐ C. Use Placement Groups and ensure that all instances are launched at the same time. ✓
- ☐ D. Use the largest EC2 instances currently available on AWS and make sure they are spread across multiple availability zones.

Explanation :

Answer – C

Option A is incorrect because being in the same region would not mean that the data transfer between the instances would be any faster. In fact, the instances would experience network latency.

Option B is incorrect because just being in the same AZ is not sufficient; they should be added to a Placement Group to benefit from the low network latency.

Option C is CORRECT because Placement Group enables applications to get the low-latency network performance necessary for tightly-coupled node-to-node communication typical of many high-performance computing applications.

Option D is incorrect because despite being of largest size, the EC2 instances would still experience network latency if they are not part of a Placement Group.



More information on Placement Groups:

A *placement group* is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking

For more information on Placement Groups, please visit the 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 2

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Due to a lot of your EC2 services going offline at least once a week for no apparent reason your security officer has told you that you need to tighten up the logging of all events that occur on your AWS account. He wants to be able to access all events that occur on the account across all regions quickly and in the simplest way possible. He also wants to make sure he is the only person that has access to these events in the most secure way possible. Which of the following would be the best solution to assure his requirements are met?

Choose the correct answer from the below options:

- ☒ A. Use CloudTrail to log all events to one S3 bucket. Make this S3 bucket only accessible by your security officer with a bucket policy that restricts access to his user only and also add MFA to the policy for a further level of security. ✓
- ☐ B. Use CloudTrail to log all events to an Amazon Glacier Vault. Make sure the vault access policy only grants access to the security officer's IP address. ^

- ☐ C. Use CloudTrail to send all API calls to CloudWatch and send an email to the security officer every time an API call is made. Make sure the emails are encrypted.
- ☐ D. Use CloudTrail to log all events to a separate S3 bucket in each region as CloudTrail cannot write to a bucket in a different region. Use MFA and bucket policies on all the different buckets.

Explanation :

Answer - A

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

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

Create Trail

Trail name*

Apply trail to all regions

☒ Yes ☐ No



Creates the same trail in all regions and delivers log files for all regions



Storage location

Create a new S3 bucket ☒ Yes ☐ No

S3 bucket*

cloudtrailbucket1



New S3 bucket where you would like your logs delivered. CloudTrail will create the bucket and apply the appropriate policy.

► Advanced

Option B is incorrect because it uses Amazon Glacier vaults which is an archival solution and not used for storing the CloudTrail logs.

Option C is incorrect because sending the API calls to CloudWatch is unnecessary. Also notifying the security officer via email is not a good nor a secure architecture.

Option D is incorrect because CloudTrail provides with an option where all the logs get delivered to a single S3 bucket. Putting all the logs in separate buckets is an overhead.

More information on AWS CloudTrail

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

You can design CloudTrail to send all logs to a central S3 bucket.

For more information on CloudTrail, please visit the below URL

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

Ask our Experts



An auditor needs read-only access to all AWS resources and logs of all the events that have occurred on AWS. What is the best way for creating this sort of access?

Choose the correct answer from the options below:

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

Explanation :

Answer – D

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

Option B is incorrect because sending the logs via email is not a good architecture.

Option C is incorrect because granting the auditor access to AWS resources is not AWS's responsibility. It is the AWS user or account owner's responsibility.

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

More information on AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a



history of AWS API calls for your account, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting. For more information on CloudTrail, please visit the below URL:
<https://aws.amazon.com/cloudtrail/> (<https://aws.amazon.com/cloudtrail/>)

Ask our Experts



QUESTION 4

UNATTEMPTED

DATA STORAGE

An online gaming server in which you have recently increased its IOPS performance, by creating a RAID 0 configuration has now started to have bottleneck problems due to your instance bandwidth. Which of the following would be the best solution for this to increase throughput?

Choose the correct answer from the below options:

- ☐ A. Use Single Root I/O Virtualization (SR-IOV) on all the instances. ✓
- ☐ B. Move all your EC2 instances to the same availability zone.
- ☐ C. Use a RAID 1 configuration instead of RAID 0.
- ☐ D. Use instance store backed instances and stripe the attached ephemeral storage devices and use DRBD Asynchronous Replication.

Explanation :

Answer - A



Option A is CORRECT because SR-IOV helps in achieving higher network throughput, lower CPU utilization, and lower network latency which can translate into supporting more VMs per host, delivering increased network bandwidth utilization on the host, and providing greater performance predictability to the instances.

Option B is incorrect because having all the instances in the same AZ does not necessarily increase the throughput.

Option C is incorrect because RAID 1 configuration which has data mirroring, provides redundancy of data for high availability; it does not increase the throughput.

Option D is incorrect because this option will help in achieving high availability, not increased throughput.

More information on SR-IOV:

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latency.

Reference Link:

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

Ask our Experts



QUESTION 5

UNATTEMPTED

NETWORK DESIGN

You are designing multi-region architecture and you want to send users to a geographic location based on latency-based routing, which seems simple enough; however, you also want to use weighted-based routing among resources within that region. Which of the below setups would best accomplish this?

Choose the correct answer from the below options:



- ☐ A. You will need to use complex routing (nested record sets) and ensure that you define the latency based records first
- ☐ B. You will need to use complex routing (nested record sets) and ensure that you define the weighted resource record sets first. ✓
- ☐ C. This cannot be done. You can't use different routing records together.
- ☐ D. You will need to use AAAA - IPv6 addresses when you define your weighted based record sets.

Explanation :

Answer – B

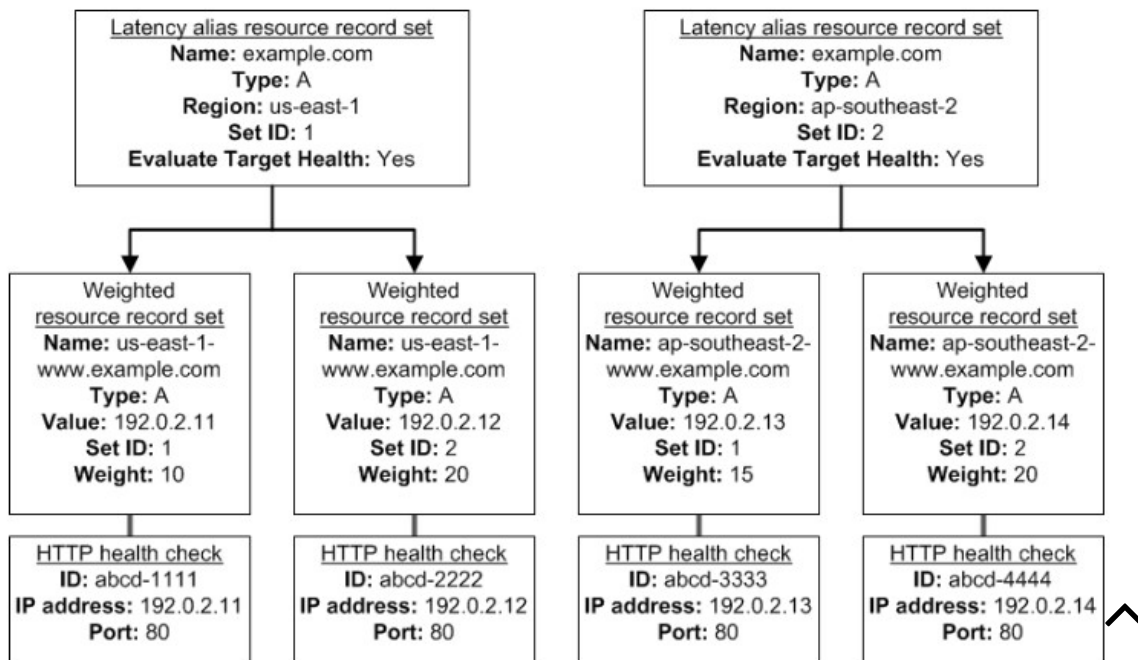
Option A is incorrect because you need to define the record set to be pointed to (in this case weighted) before creating the top level record set (in this case latency).

Option B is CORRECT because you need to create the weighted policies first because you are going to use those record sets as the alias pointing to in the latency record sets.

Option C is incorrect because you can create the nested record sets to accomplish this.

Option D is incorrect because use of IPv6 is not mandatory in this configuration (and it does not mention any latency based routing - which is one of the requirements).

Please refer to the below documentation from AWS for an example where you can define complex routing



Please find the below link for complex based routing:

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html> (<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html>)

Ask our Experts



QUESTION 6

UNATTEMPTED

COSTING

An Amazon Redshift cluster with four nodes is running 24/7/365 and expects potentially to add one on-demand node for one to two days once during the year. Which architecture would have the lowest possible cost for the cluster requirement?

Choose the correct answer from the below options:

- ☐ A. Purchase 4 reserved nodes and rely on on-demand instances for the fifth node, if required. ✓
- ☐ B. Purchase 5 reserved nodes to cover all possible usage during the year.
- ☐ C. Purchase 4 reserved nodes and bid on spot instances for the extra node if required.
- ☐ D. Purchase 2 reserved nodes and utilize 3 on-demand nodes only for peak usage times.

Explanation :

Answer - A

Option A is CORRECT because (a) the application requires 4 nodes throughout the year and reserved instances would save the cost, and (b) since the need of the other node is not assured, on-demand instance(s) can be purchased if and when needed.

Option B is incorrect because reserving 5th node is unnecessary.



Option C is incorrect because, even though the spot instances are cheaper than on-demand instances, they should only be used if the application is tolerant of sudden termination of them. Since the question does not mention this, purchasing spot instance(s) may not be a good option.

Option D is incorrect because reserving only 2 instances would not be sufficient.

Please find the below link for Reserved Instances:

<https://aws.amazon.com/ec2/pricing/reserved-instances/>
(<https://aws.amazon.com/ec2/pricing/reserved-instances/>)

Ask our Experts



QUESTION 7

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

A company has placed a set of on-premise resources with an AWS Direct Connect provider. After establishing connections to a local AWS region in the US, the company needs to establish a low latency dedicated connection to an S3 public endpoint over the Direct Connect dedicated low latency connection. What steps need to be taken to accomplish configuring a direct connection to a public S3 endpoint?

Choose the correct answer from the options given below:

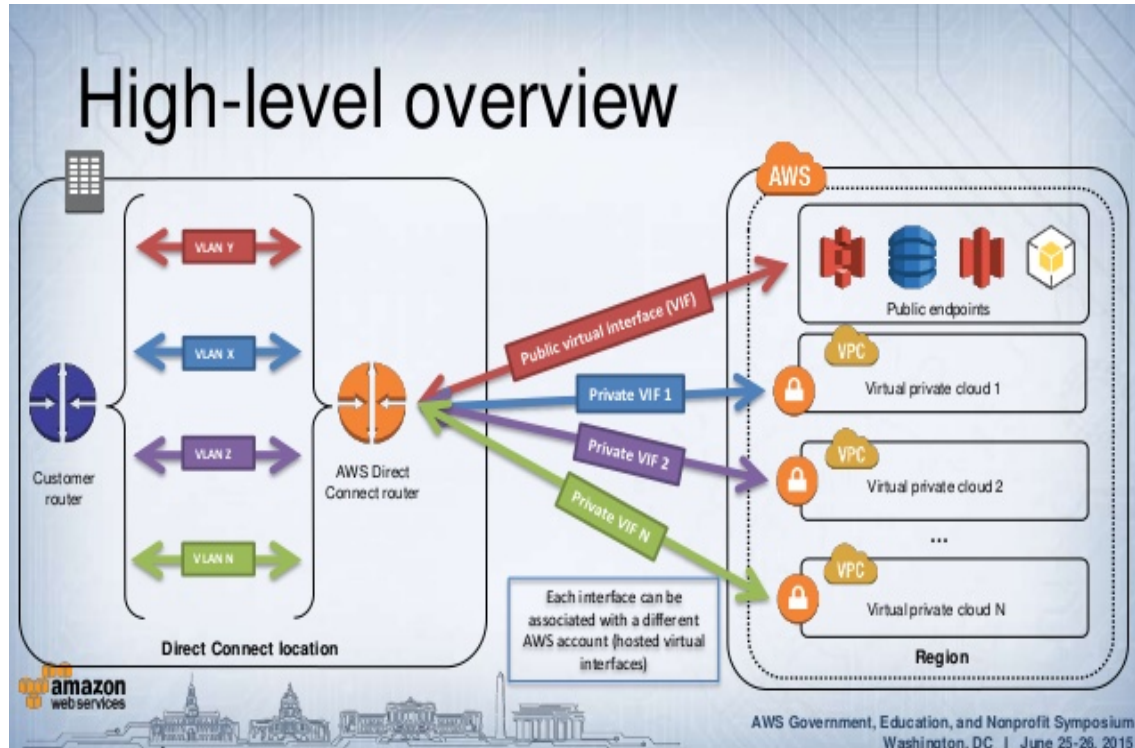
- ☐ A. Configure a public virtual interface to connect to a public S3 endpoint resource. ✓
- ☐ B. Establish a VPN connection from the VPC to the public S3 endpoint.
- ☐ C. Configure a private virtual interface to connect to the public S3 endpoint via the Direct Connect connection.
- ☐ D. Add a BGP route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

Explanation :



Answer – A

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



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

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

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

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

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

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



Ask our Experts



QUESTION 8

UNATTEMPTED

NETWORK DESIGN

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

Choose 2 options from below:

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

Explanation :

Answers – C and D



Option A is incorrect because (a) NAT instance is ideally used to route traffic from a private subnet to the internet via a public subnet, (b) NAT instance is not managed by AWS and requires to be configured and maintained by the user; hence, adding to the overhead, and (c) if not scaled, can cause performance bottleneck. NAT Gateway is a preferred option over NAT instances.

Option B is recommending us to use AWS CloudFront and configure the distributions Origin to the web server and then use a AWS Route 53 'CNAME' for the CloudFront Distribution. Even though CloudFront is highly available and is accessible to the Internet, it would work better if the Origin for the AWS CloudFront Distribution was pointed to an AWS ELB rather than to the Web Server itself. 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 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, (b) In Route53, you can either resolve the DNS query via creating an ALIAS record pointing to the ELB endpoint or an A record pointing to the IP Addresses of the application. As the EIPs are static (will not be changed) and can be assigned to new web servers if any of the web servers becomes offline, the EIPs can be used in the A record. The health check would ensure that Route53 checks the health of the record set before the failover to other web servers.



Create Record Set

Name: .awssampletest.com.

Type:

Alias: ☐ Yes ☒ No

TTL (Seconds):

Value:
54.173.104.79
34.226.150.123

IPv4 address. Enter multiple addresses
on separate lines.

Example:

192.0.2.235


198.51.100.234

Routing Policy:

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

Failover Record Type: ☒ Primary ☐ Secondary

Set ID:

Associate with Health Check: ☒ Yes ☐ No 

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

Health Check to Associate:

Ask our Experts





QUESTION 9

UNATTEMPTED

DATA STORAGE

You have launched an EC2 instance with four (4) 500 GB EBS Provisioned IOPS volumes attached. The EC2 instance is EBS-Optimized and supports 500 Mbps throughput between EC2 and EBS. The EBS volumes are configured as a single RAID 0 device, and each Provisioned IOPS volume is provisioned with 4,000 IOPS (4,000 16KB reads or writes) for a total of 16,000 random IOPS on the instance. The EC2 instance initially delivers the expected 16,000 IOPS random read and write performance. Sometime later in order to increase the total random I/O performance of the instance, you add an additional two 500 GB EBS Provisioned IOPS volumes to the RAID. Each volume is provisioned to 4,000 IOPS like the original four for a total of 24,000 IOPS on the EC2 instance. Monitoring shows that the EC2 instance CPU utilization increased from 50% to 70%. but the total random IOPS measured at the instance level did not increase at all. What is the problem and a valid solution?

- ☐ A. Larger storage volumes support higher Provisioned IOPS rates; hence, increase the provisioned volume storage of each of the 6 EBS volumes to 1TB.
- ☐ B. The EBS-Optimized throughput limits the total IOPS that can be utilized; hence, use an EBS-Optimized instance that provides larger throughput. ✓
- ☐ C. Small block sizes cause performance degradation, limiting the I/O throughput; hence, configure the instance device driver and file system to use 64KB blocks to increase throughput.
- ☐ D. RAID 0 only scales linearly to about 4 devices, use RAID 0 with 4 EBS Provisioned IOPS volumes but increase each Provisioned IOPS EBS volume to 6,000 IOPS.



- E. The standard EBS instance root volume limits the total IOPS rate; hence, change the instant root volume to also be a 500GB 4,000 Provisioned IOPS volume.

Explanation :

Answer - B

Option A is incorrect because increasing the volume size may not be sufficient; you will not get the higher IOPS unless the volumes are attached to EBS-optimized instance types with larger throughput (e.g. 8xlarge or higher).

Option B is CORRECT because EC2 Instance types have limit on max throughput and would require 8xlarge or higher instance types to provide 24000 or more IOPS.

Option C is incorrect because this option will not increase the IOPS.

Option D is incorrect because the reasoning given for the issue (RAID 0 only scaling for 4 volumes) is not true.

Option E is incorrect because it already has sufficient number of volumes with 4,000 PIOPS attached. So, changing the root volume to a 4,000 PIOPS will not be useful.

More information on the topic from AWS documentation:

Launching an instance that is EBS-optimized provides you with a dedicated connection between your EC2 instance and your EBS volume. However, it is still possible to provision EBS volumes that exceed the available bandwidth for certain instance types, especially when multiple volumes are striped in a RAID configuration. Be sure to choose an EBS-optimized instance that provides more dedicated EBS throughput than your application needs; otherwise, the Amazon EBS to Amazon EC2 connection will become a performance bottleneck.

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

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

"In order to get the most performance out of your EBS volumes, you should attach them to an instance with enough bandwidth to support your volumes, such as an EBS-optimized instance or an instance with 10 Gigabit network connectivity. This is especially important when you stripe multiple volumes together in a RAID configuration."



Ask our Experts



QUESTION 10

UNATTEMPTED

SCALABILITY & ELASTICITY

Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS. Which service should you use?

- ☐ A. Amazon RDS with provisioned IOPS up to the anticipated peak write throughput.
- ☐ B. Amazon Simple Queue Service (SQS) for capturing the writes and draining the queue to write to the database. ✓
- ☐ C. Amazon ElastiCache to store the writes until the writes are committed to the database.
- ☐ D. Amazon DynamoDB with provisioned write throughput up to the anticipated peak write throughput.

Explanation :

Answer - B

Option A and D are incorrect because the peak amount of traffic is undetermined; so you cannot provision the "provisioned IOPS" beforehand.

Option B is CORRECT because SQS is AWS managed and highly scalable service that can hold the database write requests in the queue, and ensure that no writes will be dropped.

Option C is incorrect because ElastiCache is used for read-heavy applications to reduce the load on the database (not to cache the writes).

For more information on SQS, please read the related questions in the FAQs

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



Ask our Experts



QUESTION 11

UNATTEMPTED

SECURITY

As an IT administrator, you have been tasked to develop a reliable and durable logging solution to track changes made to your EC2, IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log data. Which of these solutions would you implement?

- ☐ **A.** Create a new cloud trail with one new S3 bucket to store the logs and with the global services option selected. Use IAM Roles, Bucket policies and MFA Delete for ensuring additional authentication for deleting objects from S3 buckets. ✓
- ☐ **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

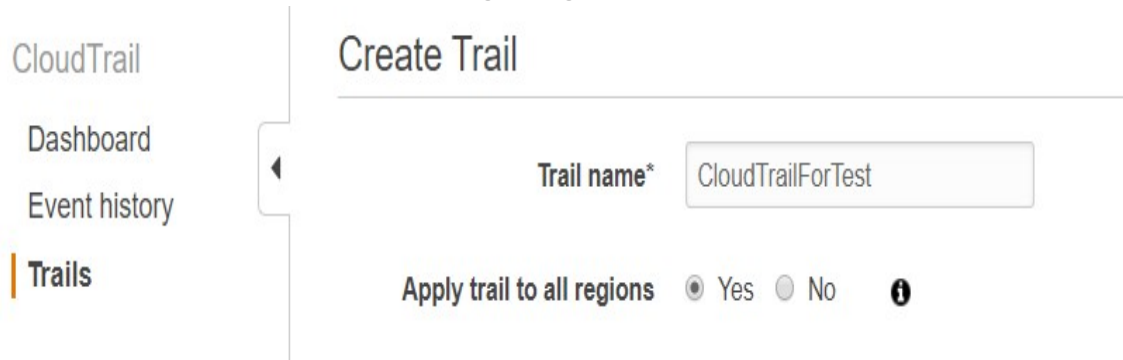
For the scenarios where the application is tracking (or needs to track) the changes made by any AWS service, resource, or API, always think about AWS CloudTrail service.



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 option to apply the trail to all regions (global).



Options B is incorrect because (a) although it uses AWS CloudTrail, the Global Option is not enabled, and (b) SNS notifications can be an 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



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

Choose the correct answer from the below options:

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

Explanation :

Answer – D

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

Option A is incorrect because embedding keys in the application to access AWS resource is not a good architectural practice as it creates security concerns.

Option B is incorrect because HSM certificate is used by Redshift cluster to connect to the client's HSM in order to store and retrieve the keys used to encrypt the cluster databases.

Option C is incorrect because read-only policy is insufficient and embedding keys in the application to access AWS resource is not a good architectural practice as it creates security concerns.

Option D is CORRECT because (a) IAM role allows the least privileged access to the AWS resource, (b) web identity federation ensures the identity of the user, and (c) the user is given temporary credentials to access the AWS resource.

For more information on IAM policies please refer to the below link:



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

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

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

For more information on web identity federation please refer to the below link

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

Ask our Experts



QUESTION 13

UNATTEMPTED

SECURITY

Which of the following must be done while generating a pre-signed URL in S3 in order to ensure that the user who is given the pre-signed URL has the permission to upload the object?

- ☐ A. Ensure the user has write permission to S3.
- ☐ B. Ensure the user has read permission to S3.
- ☐ C. Ensure that the person who has created the pre-signed URL has the permission to upload the object to the appropriate S3 bucket. ✓
- ☐ D. Create a Cloudfront distribution.

Explanation :

Answer - C



Option A is incorrect because if the person who has created the pre-signed URL does not have write permission to S3, the person who is given the pre-signed URL will not have it either.

Option A is incorrect because if the person who has created the pre-signed URL does not have read permission to S3, the person who is given the pre-signed URL will not have it either.

Option C is CORRECT because in order to successfully upload an object to S3, the pre-signed URL must be created by someone who has permission to perform the operation that the pre-signed URL is based upon.

Option D is incorrect because CloudFront distribution is not needed in this scenario.

For more information on pre-signed URL's, please visit the below URL

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

Ask our Experts



QUESTION 14

UNATTEMPTED

COSTING

A customer needs corporate IT governance and cost oversight of all AWS resources consumed by its divisions. The divisions want to maintain administrative control of the discrete AWS resources they consume and keep those resources separate from the resources of other divisions. Which of the following options, when used together, will support the autonomy/control of divisions while enabling corporate IT to maintain governance and cost oversight? Choose 2 answers

- ☐ A. Use the consolidated billing feature in AWS Organizations to consolidate payment for multiple AWS accounts. ✓
- ☐ B. Create separate VPC's for each divisions with in the AWS account



- ☐ C. Write all child AWS CloudTrail and Cloudwatch logs to each child account's Amazon S3 IA
- ☐ D. Enable AWS Organizations's "all features" in your organization. ✓
- ☐ E. Write all child AWS CloudTrail and Amazon CloudWatch logs to each child account's Amazon S3 'Log' bucket.

Explanation :

Answers - A & D

We need to satisfy 2 requirements here.

1. To provide either autonomy or control of divisions while maintaining IT Governance
2. To evaluate the overall cost

AWS Organizations has two available feature sets: **consolidated billing features and all features**. All organizations support consolidated billing, which provides basic management tools that you can use to centrally manage the accounts in your organization.

If you enable **all features**, you continue to get all the consolidated billing features plus a set of advanced features such as service control policies (SCPs), which give you fine-grained control over which services and actions that member accounts can access.

When you start the process to enable all features, AWS Organizations sends a request to every member account that you *invited* to join your organization. Every invited account must approve enabling all features by accepting the request. Only then can you complete the process to enable all features in your organization. If an account declines the request, you must either remove the account from your organization or resend the request and get it accepted before you can complete the process to enable all features. Accounts that you *created* using AWS Organizations don't get a request because they don't need to approve the additional control.

- <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>

(<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>)

- https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html



(https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html)

With options B&C the two requirements of the scenario are not met.

Ask our Experts



QUESTION 15

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A user has launched a large EBS backed EC2 instance in the US-East-1 region. The user wants to achieve Disaster Recovery (DR) for that instance by creating another small instance in Europe. How can the user achieve DR?

- ☐ A. Copy the running instance using the “Instance Copy” command to the EU region.
- ☐ B. Create an AMI of the instance and copy the AMI to the EU region. Then launch the instance from the EU AMI. ✓
- ☐ C. Copy the instance from the US East region to the EU region.
- ☐ D. Use the “Launch more like this” option to copy the instance from one region to another.

Explanation :

Answer – B

Option A and C are incorrect because you cannot directly copy the instance. You need to create AMI of each instance.

Option B is CORRECT because if you need an AMI across multiple regions, then you have to copy the AMI across regions. Note that by default AMI's that you have created will not be available across all regions. ^

Option D is incorrect because using "Launch More Like This..." enables you to use a current instance as a base for launching other instances in the same availability zone. It does not clone your selected instance; it only replicates some configuration details. To create a copy of your instance, first create an AMI from it, then launch more instances from the AMI.

For the entire details to copy AMI's, please visit the link -

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

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

Ask our Experts



QUESTION 16

UNATTEMPTED

SCALABILITY & ELASTICITY

A user has setup Auto Scaling with ELB on the EC2 instances. The user wants to configure that whenever the CPU utilization is below 10%, Auto Scaling should remove one instance. How can the user configure this?

- ☐ A. The user can get an email using SNS when the CPU utilization is less than 10%. The user can use the desired capacity of Auto Scaling to remove the instance.
- ☐ B. Use CloudWatch to monitor the data and Auto Scaling to remove the instances using scheduled actions.
- ☐ C. Configure a CloudWatch alarm in the execution policy that notifies the Auto Scaling Launch configuration when the CPU utilization is less than 10%, and configure the Auto Scaling policy to remove the instance.
- ☐ D. Configure a CloudWatch alarm in the execution policy that notifies the Auto Scaling group when the CPU Utilization is less than 10%, and configure the Auto Scaling policy to remove the instance. ✓

Explanation :



Answer – D

Option A is incorrect because for the user to get the notification, they have to configure CloudWatch which triggers a notification to Auto Scaling Group to terminate the instance. Updating the desired capacity will not work in this case.

Option B is incorrect because scheduled scaling is used to scale your application in response to predictable load changes, not upon any notification.

Option C is incorrect because the notification should be sent to Auto Scaling Group, not the launch configuration.

Option D is CORRECT because the notification is sent to Auto Scaling Group which then removes an instance from the running instances.

More information on Auto Scaling, Scheduled Actions:

Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your desired number of Amazon EC2 instances. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.

For more information on AutoScaling, please visit the link –

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

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

(https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html)

Ask our Experts



QUESTION 17

UNATTEMPTED

COSTING

An organization has added 3 of his AWS accounts to consolidated billing. One of the AWS accounts has purchased a Reserved Instance (RI) of a small instance size in the US-East-1a zone. All other AWS accounts are running instances of a small size in the same zone. What will happen in this case for the RI pricing?



- ☐ A. Only the account that has purchased the RI will get the advantage of RI pricing.
- ☐ B. One instance of a small size and running in the US-East-1a zone of each AWS account will get the benefit of RI pricing.
- ☐ C. Any single instance from all the three accounts can get the benefit of AWS RI pricing if they are running in the same zone and are of the same size. ✓
- ☐ D. If there are more than one instances of a small size running across multiple accounts in the same zone no one will get the benefit of RI.

Explanation :

Answer – C

Option A is incorrect because the price benefit of the reserved instances is applicable to all the accounts that are part of the consolidated billing group, not just the payer account (or the account that has reserved the instance) - for the total number of instances reserved.

Option B is incorrect because, since only a single instance is reserved, any one instance across all the accounts will receive the reserved instance price benefit.

Option C is CORRECT because the reserved price benefit will be applied to a single EC2 instance across all the accounts.

Option D is incorrect because the total number of instances that will receive the cost benefit will be same as the total number of reserved instances (in this case it's one).

More information on Consolidated Billing:

As per the AWS documentation for billing purposes, AWS treats all the accounts on the consolidated bill as if they were one account. Some services, such as Amazon EC2 and Amazon S3, have volume pricing tiers across certain usage dimensions that give you lower prices when you use the service more. With consolidated billing, AWS combines the usage from all accounts to determine which volume pricing tiers to apply, giving you a lower overall price whenever possible.

For more information on Consolidated billing, please visit the URL:

<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>
(<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html>)

Ask our Experts



A user has configured an SSL listener at ELB as well as on the back-end instances. Which of the below-mentioned statements helps the user understand ELB traffic handling with respect to the SSL listener?

- ☐ A. It is not possible to have the SSL listener both at ELB and back-end instances.
- ☐ B. ELB will modify headers to add requestor details.
- ☐ C. ELB will intercept the request to add the cookie details if sticky session is enabled.
- ☐ D. ELB will not modify the headers. ✓

Explanation :

Answer – D

Option A is invalid because if the front-end connection uses TCP or SSL, then your back-end connections can use either TCP or SSL. If the front-end connection uses HTTP or HTTPS, then your back-end connections can use either HTTP or HTTPS.

Option B is invalid because when you use TCP/SSL for both front-end and back-end connections, your load balancer forwards the request to the back-end instances without modifying the headers.

Option C is invalid because with this configuration you do not receive cookies for session stickiness. But, when you use HTTP/HTTPS, you can enable sticky sessions on your load balancer.

Option D is CORRECT because with SSL configuration, the load balancer will forward the request to the back-end instances without modifying the headers.

For more information on ELB, please visit the link:

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

Ask our Experts



A user is using CloudFormation to launch an EC2 instance and then configure an application after the instance is launched. The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly. How can the user configure this?

- ☐ A. It is not possible that the stack creation will wait until one service is created and launched.
- ☐ B. The user can use the HoldCondition resource to wait for the creation of the other dependent resources.
- ☐ C. The user can use the DependentCondition resource to hold the creation of the other dependent resources.
- ☐ D. The user can use the WaitCondition resource to hold the creation of the other dependent resources. ✓

Explanation :

Answer – D

You can use a wait condition for situations like the following:

- To coordinate stack resource creation with configuration actions that are external to the stack creation
- To track the status of a configuration process

For more information on CloudFormation Wait condition please visit the link

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html>

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

Ask our Experts



An organization has created one IAM user and applied the below-mentioned policy to the user. What entitlements do the IAM users avail with this policy?

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "VisualEditor0",  
      "Effect": "Allow",  
      "Action": [  
        "ec2:Describe*"  
      ],  
      "Resource": "*"  
    },  
    {  
      "Sid": "VisualEditor0",  
      "Effect": "Allow",  
      "Action": [  
        "autoscaling:Describe*"  
      ],  
      "Resource": "*"  
    },  
    {  
      "Sid": "VisualEditor0",
```




```
"Effect": "Allow",  
"Action": [  
    "cloudwatch:ListMetrics",  
    "cloudwatch:Describe*",  
    "cloudwatch:GetMetricStatistics"  
],  
"Resource": "*" ]  
}
```

- ☐ A. The policy will allow the user to perform all read-only activities on the EC2 services.
- ☐ B. The policy will allow the user to list all the EC2 resources except EBS.
- ☐ C. The policy will allow the user to perform all read and write activities on the EC2 services.
- ☐ D. The policy will allow the user to perform all read-only activities on the EC2 services except load Balancing. ✓

Explanation :

Answer – D

AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If an organization wants to setup read only access to EC2 for a particular user, they should mention the action in the IAM policy which entitles the user for Describe rights for EC2, CloudWatch, Auto Scaling and ELB. In the policy shown below, the user will have read only access for EC2, CloudWatch and Auto Scaling. Since ELB is not mentioned as a part of the list, the user will not have access to ELB.

The above policy will allow the user to view EC2 instances, look at AutoScaling and CloudWatch but not allow the user access to Load Balancing. For the access to load balancing, you need to add the following statements as well.



```
"Effect": "Allow",  
"Action": "elasticloadbalancing:Describe*",  
"Resource": "*"
```

For more information on IAM policy , please visit the URL:

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

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

Ask our Experts



QUESTION 21

UNATTEMPTED

NETWORK DESIGN

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user's data center. The user's data center has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-12345) to allow traffic to the internet from the VPN subnet. Which of the below-mentioned options is not a valid entry for the main route table in this scenario?

- ☐ A. Destination: 20.0.1.0/24 and Target: i-12345 ✓
- ☐ B. Destination: 0.0.0.0/0 and Target: i-12345
- ☐ C. Destination: 172.28.0.0/12 and Target: vgw-12345
- ☐ D. Destination: 20.0.0.0/16 and Target: local

Explanation :

Answer – A

Option A is CORRECT because the destination of private subnet with NAT instance as target is not needed in the route table. This is an invalid entry.

Option B is incorrect because you would need this entry to be able to communicate with the

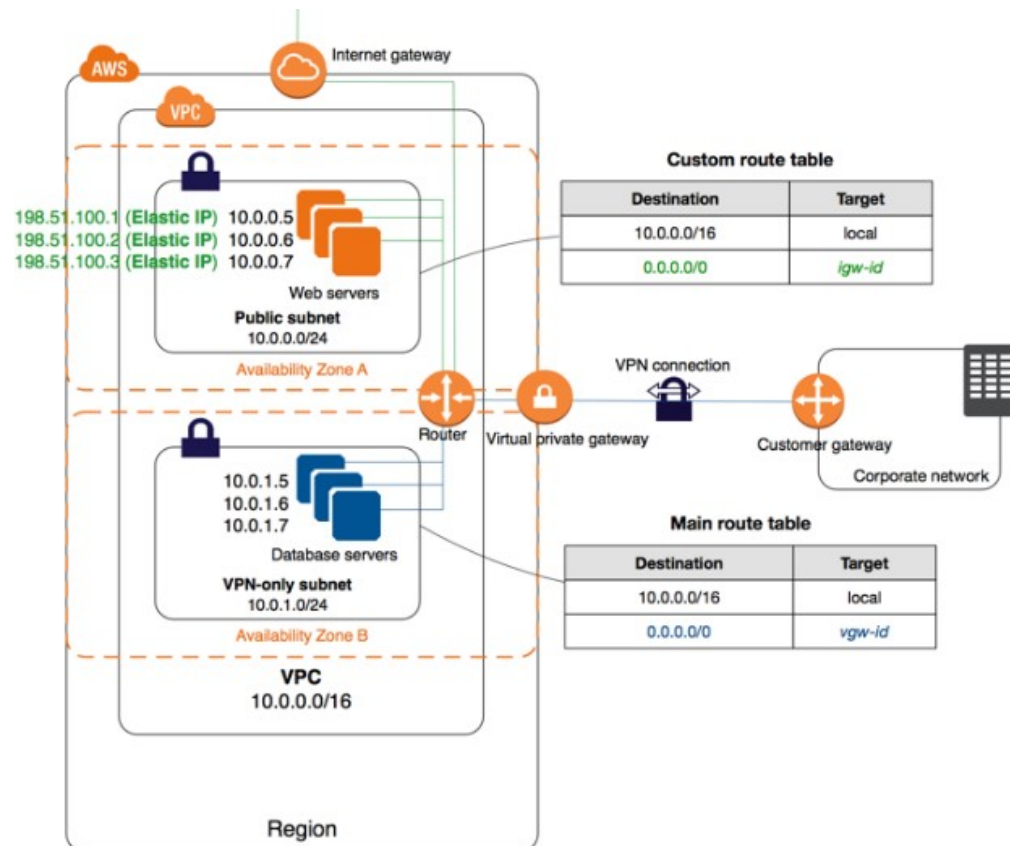


internet via NAT instance (e.g. for patch updates).

Option C is incorrect because you need this entry for communicating with customer network via the virtual private gateway.

Option D is incorrect because this entry is present by default to allow the resources in the VPC to communicate with each other.

The below diagram shows how a typical setup for a VPC with VPN and Internet gateway would look like. The only routing option which should have access to the internet gateway should be the 0.0.0.0/0 address. So Option A is the right answer.



For more information on VPC with the option of VPN, please visit the link http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html)

Ask our Experts



An organization has configured Auto Scaling with ELB. There is a memory issue in the application which is causing CPU utilization to go above 90%. The higher CPU usage triggers an event for Auto Scaling as per the scaling policy. If the user wants to find the root cause inside the application without triggering a scaling activity, how can he achieve this?

- ☐ A. Stop the scaling process until research is completed.
- ☐ B. It is not possible to find the root cause from that instance without triggering scaling.
- ☐ C. Delete AutoScaling group until research is completed.
- ☒ D. Suspend the scaling process until research is completed. ✓

Explanation :

Answer – D

In this scenario, the user wants to investigate the problem during the AutoScaling process without triggering the scaling activity. For this, the user can leverage the suspend and resume option available on AutoScaling.

Option A is incorrect because the scaling process need not be stopped, it can be suspended so that it can be resumed.

Option B is incorrect because scaling can be momentarily suspended until the investigation is completed.

Option C is incorrect because AutoScaling group is totally unnecessary in this scenario.

Option D is CORRECT because you can suspend and then resume one or more of the scaling processes for your Auto Scaling group if you want to investigate a configuration problem or other issue with your web application and then make changes to your application, without triggering the scaling processes.

For more information on suspending AutoScaling processes, please visit the link <http://docs.aws.amazon.com/autoscaling/latest/userguide/as-suspend-resume-processes.html> (<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-suspend-resume-processes.html>)



Ask our Experts



QUESTION 23

UNATTEMPTED

SECURITY

A company has 2 accounts- one is a development account and the other is the production account. There are 20 people on the development account who now need various levels of access provided to them on the production account. 10 of them need read-only access to all resources on the production account, 5 of them need read/write access to EC2 resources, and the remaining 5 only need read-only access to S3 buckets. Which of the following options would be the best way for both practically and security-wise to accomplish this task?

Choose the correct answer from the below options:

- ☐ **A.** Create 3 roles in the production account with a different policy for each of the access levels needed. Add permissions to each IAM User on the developer account based on the type of access needed. ✓
- ☐ **B.** Create 3 new users on the production account with the various levels of permissions needed. Give each of the 20 users the login for whichever one of the 3 users they need depending on the level of access required.
- ☐ **C.** Create encryption keys for each of the resources that need access and provide those keys to each user depending on the access required.
- ☐ **D.** Copy the 20 users IAM accounts from the development account to the production account. Then change the access levels for each user on the production account.

Explanation :

Answer - A



Option A is CORRECT because it creates 3 roles according to the need inside the production account and adds the permissions to each of the IAM User in development account to assume those roles accordingly.

Option B is incorrect because you should be creating IAM Roles in the production account and the development users should assume those roles. This option is suggesting to create 3 separate users in production account which is incorrect.

Option C is incorrect because creation of encryption keys is totally unnecessary and will not work in this scenario.

Option D is incorrect because creation of the IAM user accounts in the production account is unnecessary. You should be creating IAM Roles instead.

For more information on "Delegating Access Across AWS Accounts Using IAM Role" - please refer to the below link:

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

Ask our Experts



QUESTION 24

UNATTEMPTED

SECURITY

A user has created a mobile application which makes calls to DynamoDB to fetch certain data. The application is using the DynamoDB SDK and root account access/secret access key to connect to DynamoDB from mobile. Which of the below-mentioned statements is true with respect to the best practice for security in this scenario?

- ☐ A. The user should create a separate IAM user for each mobile application and provide DynamoDB access with it.
- ☐ B. The user should create an IAM role with DynamoDB and EC2 access. Attach the role with EC2 and route all calls from the mobile through EC2.



- ☐ C. The application should use an IAM role with web identity federation which validates calls to DynamoDB with identity providers, such as Google, Amazon, and Facebook. ✓
- ☐ D. Create an IAM Role with DynamoDB access and attach it with the mobile application.

Explanation :

Answer – C

Option A is incorrect because creating a separate user for each application user is not a feasible, secure, and recommended solution.

Option B is incorrect because the mobile users may not all be AWS users. You need to give access to the mobile application via federated identity provider.

Option C is CORRECT because it creates a role for Federated Users which enables the users to sign in to the app using their Amazon, Facebook, or Google identity and authorize them to seamlessly access DynamoDB.

Option D is incorrect because creating IAM Role is not sufficient. You need to authenticate the users of the application via web identity provider, then get the temporary credentials via a Security Token Service (STS) and then access DynamoDB.

More information on Web Identity Federation:

With Web Identity Federation, you don't need to create custom sign-in code or manage your own user identities. Instead, users of your app can sign in using a well-known identity provider (IdP) –such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account.

For more information on Web Identity Federation, please visit the 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



A user has launched an EC2 instance store-backed instance in the us-east-1a zone. The user created AMI #1 and copied it to the eu-west-1 region. After that, the user made a few updates to the application running in the us-east-1a zone. The user makes an AMI #2 after the changes. If the user launches a new instance in Europe from the AMI #1 copy, which of the below-mentioned statements is true?

- ☐ A. The new instance will have the changes made after the AMI copy as AWS just copies the reference of the original AMI during the copying. Thus, the copied AMI will have all the updated data.
- ☐ B. The new instance will have the changes made after the AMI copy since AWS keeps updating the AMI.
- ☐ C. It is not possible to copy the instance store backed AMI from one region to another.
- ☐ D. The new instance in the eu-west-1 region will not have the changes made after the AMI copy. ✓

Explanation :

Answer – D

Option A is incorrect because (a) the changes made to the instance will not automatically get updated in the AMI in US-East-1, and (b) the already copied AMI will not have any reference to the AMI in the US-East-1 region.

Option B is incorrect because AWS does not automatically update the AMIs. It needs to be done manually.

Option C is incorrect because you can copy the instance store AMI between different regions.

Option D is CORRECT because the instance in the EU region will not have any changes made after copying the AMI. You will need to copy the AMI#2 to eu-west-1 and then launch the instance again to have all the changes.

For the entire details to copy AMI's, please visit the link –

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



Ask our Experts



QUESTION 26

UNATTEMPTED

NETWORK DESIGN

A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet with port 80 and a Database server in the private subnet with port 3306. The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below-mentioned entries is required in the private subnet database security group DBSecGrp?

- ☐ A. Allow Inbound on port 3306 for the source Web Server Security Group WebSecGrp. ✓
- ☐ B. Allow Inbound on port 3306 from source 20.0.0.0/16.
- ☐ C. Allow Outbound on port 3306 for destination Web Server Security Group WebSecGrp.
- ☐ D. Allow Outbound on port 80 for destination NAT instance IP.

Explanation :

Answer – A

The important point in this question is to allow the incoming traffic to the private subnet on port 3306 only for the instances in the private subnet.

Option A is CORRECT because (a) it allows the inbound traffic only for the required port 3306, and (b) it allows only the traffic from the instances in the public subnet (WebSecGrp).

Option B is incorrect because it is allowing the inbound traffic to all the instances in the VPC which is not the requirement.



Option C is incorrect because defining outbound traffic will not ensure the incoming traffic from the public subnet. Also, since the security groups are stateful, you just need to define the inbound traffic for the public subnet only (WebSecGrp). The outbound traffic would be automatically allowed.

Option D is incorrect because you do not need to open the port 80 in this case.

More information on Web Server and DB Server Security Group settings:

Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the AWS documentation shows how the security groups should be set up.

DBServerSG: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comments
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).

For more information on security groups please visit the below link

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

Ask our Experts



An organization (Account ID 123412341234). has attached the below-mentioned IAM policy to a user. What does this policy statement entitle the user to perform?

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowUsersAllActionsForCredentials",
    "Effect": "Allow",
    "Action": [
      "iam:*LoginProfile",
      "iam:*AccessKey*",
      "iam:*SigningCertificate*"
    ],
    "Resource": ["arn:aws:iam::123412341234:user/${aws:username}"]
  }]
}
```

- ☐ A. The policy allows the IAM user to modify all IAM user's credentials using the console, SDK, CLI or APIs.
- ☐ B. The policy will give an invalid resource error.
- ☐ C. The policy allows the IAM user to modify all credentials using only the console.
- ☐ D. The policy allows the user to modify the IAM user's password, sign in certificates and access keys only. ✓

Explanation :

Answer – D



First, in order to give a user a certain set of policies, you need to mention the following line.
The aws:username will apply to the AWS logged in user.

Resource": "arn:aws:iam::*account-id-without-hyphens*.user/\${aws:username}

Next, the policies will give the permissions to modify the IAM user's password, sign in certificates and access keys

"iam:*LoginProfile",

"iam:*AccessKey*",

"iam:*SigningCertificate"

For information on IAM security policies, please visit the link:

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

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

Ask our Experts



QUESTION 28

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 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:



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 x

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 ⓘ

Create Auto Scaling Group

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 ⓘ

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 Demo. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency.

[Learn more](#)

Instance Protection ⓘ

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 29

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 answers from the below options:

- ☐ A. A network ACL that allows communication between the two subnets. ✓
- ☐ 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. Security groups are set to allow the application host to talk to the database on the right port/protocol. ✓

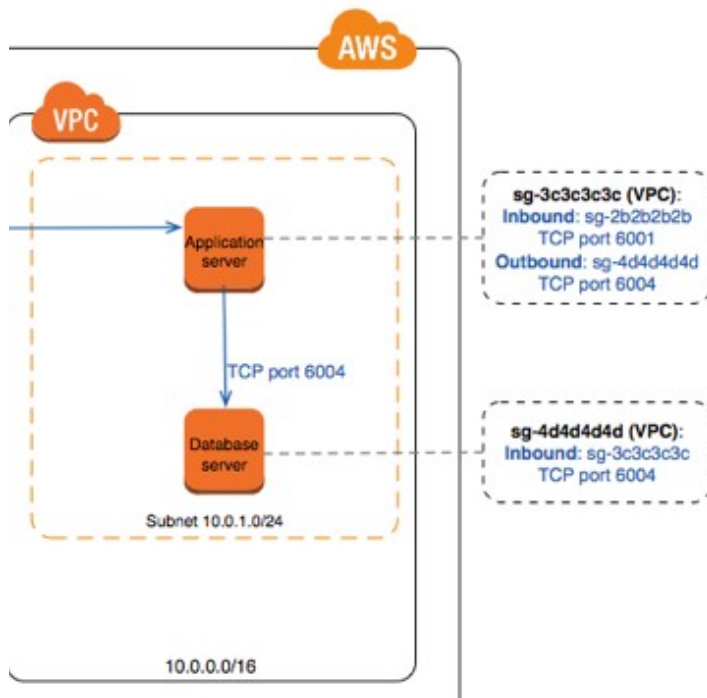
Explanation :

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:



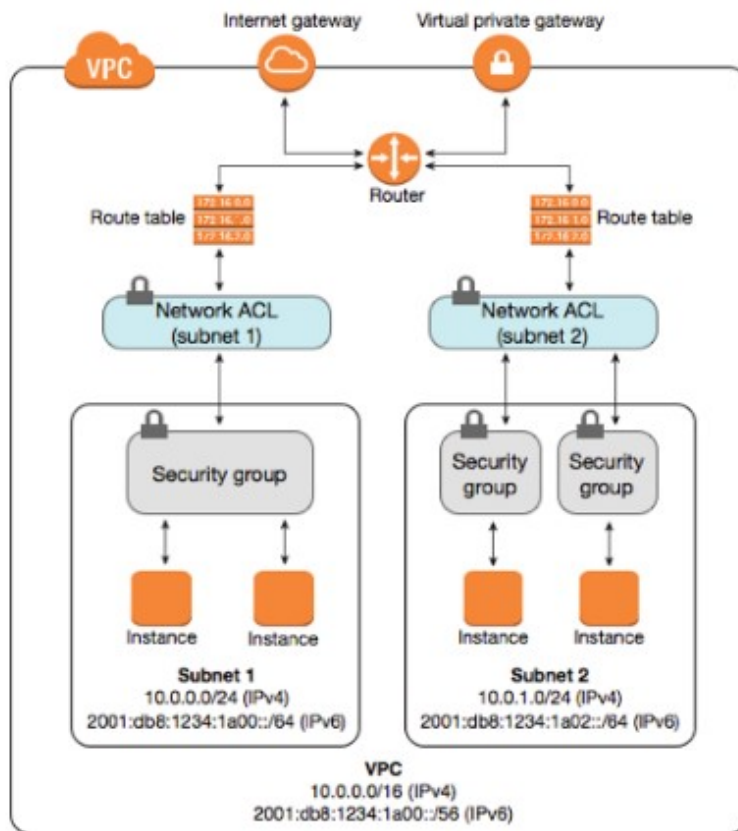


Option B is incorrect because it is not necessary to have the two instances of the same type or be using same key-pair.

Option C incorrect is 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



QUESTION 30

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 . 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 invalid as Cost allocation reports are used to set up and customize monthly *cost allocation report* for your *AWS* usage to see meaningful billing information that helps you track your costs. Only AWS Opsworks for Chef automate or AWS OpsWorks for Puppet Enterprise can provide the version control. Hence this is not an optimal choice.

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 31

UNATTEMPTED

DEPLOYMENT MANAGEMENT

What are some of the best practices when managing permissions for OpsWorks?

Choose 3 answers from the below options:

- ☐ A. Create IAM User for each of your users and attach policies that provide appropriate access. ✓
- ☐ B. Use the root account for managing the resources attached to OpsWorks.
- ☐ C. Application developers need to access only the stacks that run their applications. ✓
- ☐ D. Users should only have access permission to the resources they need as part of the OpsWorks stack. ✓

Explanation :

Answer – A, C, and D

Option A is CORRECT because instead of using root credentials, it is a better practice is to create an IAM User with appropriate policies attached to it.

Option B is incorrect because using the root account credentials is not a secure and recommended practice.

Option C is CORRECT because developers should not have access to stacks pertaining to any other applications than the ones they should be working on.

Option D is CORRECT because users should have access to only those resources that pertain to the application they are working on.

For more information on OpsWorks best practices, please visit the link –



<http://docs.aws.amazon.com/opsworks/latest/userguide/best-practices-permissions.html>
(<http://docs.aws.amazon.com/opsworks/latest/userguide/best-practices-permissions.html>)

Ask our Experts



QUESTION 32

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Which of the following are best practices that need to be followed when updating Opswork stack instances with the latest security patches?

Choose 2 correct options from the below:

- ☐ A. Create and start new instances to replace your current online instances.
✓
- ☐ B. run the Update Dependencies stack command for Linux based instances.
✓
- ☐ C. Delete the entire stack and create a new one.
- ☐ D. Use Cloudformation to deploy the security patches.

Explanation :

Answers: A and B

The best practices for updating your OpsWork stacks instances with the latest security patches:

- Create and start new instances to replace your current online instances. Then delete the current instances. The new instances will have the latest set of security patches installed during setup.



- On Linux-based instances in Chef 11.10 or older stacks, run the Update Dependencies stack command which installs the current set of security patches and other updates on the specified instances.

For more information on OpsWork Linux security updates best practices, please visit the link –

<https://docs.aws.amazon.com/opsworks/latest/userguide/workingsecurity-updates.html>
(<https://docs.aws.amazon.com/opsworks/latest/userguide/workingsecurity-updates.html>)

Ask our Experts



QUESTION 33

UNATTEMPTED

DEPLOYMENT MANAGEMENT

While managing your instances in the current Opswork stack, you suddenly started getting the following error:

ws::CharlieInstanceService::Errors::UnrecognizedClientException - The security token included in the request is invalid.

Which of the below 2 check can be done to rectify this error?

- ☐ A. Check the IAM role which was attached to the instance. ✓
- ☐ B. Check if the EIP have been added to the EC2 instances manually. ✓
- ☐ C. Check if the stack is configured properly.
- ☐ D. Check if the Opswork client is configured properly.

Explanation :

Answer: A and B.



This can occur if a resource outside AWS OpsWorks on which the instance depends was edited or deleted. The following are examples of resource changes that can break communications with an instance.

- An IAM user or role associated with the instance has been deleted accidentally, outside of AWS OpsWorks Stacks. This causes a communication failure between the AWS OpsWorks agent that is installed on the instance and the AWS OpsWorks Stacks service. The IAM user that is associated with an instance is required throughout the life of the instance.
- Editing volume or storage configurations while an instance is offline can make an instance unmanageable.
- Adding EC2 instances to an EIP manually. AWS OpsWorks reconfigures an assigned Elastic Load Balancing load balancer each time an instance enters or leaves the online state. AWS OpsWorks only considers instances it knows about to be valid members; instances that are added outside of AWS OpsWorks, or by some other process, are removed. Every other instance is removed.

For more information on troubleshooting Opswork, please visit the link:

<http://docs.aws.amazon.com/opsworks/latest/userguide/common-issues-troubleshoot.html> (<http://docs.aws.amazon.com/opsworks/latest/userguide/common-issues-troubleshoot.html>)

Ask our Experts



QUESTION 34

UNATTEMPTED

SECURITY

There is a requirement for an application hosted on AWS to work with DynamoDB tables. The user is trying to access the application using a mobile app by using facebook credentials. Which of the following is the best option for the application hosted on an EC2 instance to work with the data in the DynamoDB table? Choose the correct answer from the options given below.

- ☐ A. Create an IAM user and assign the IAM user to a group with proper permissions to communicate with DynamoDB.



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

Explanation :

Answer - C

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

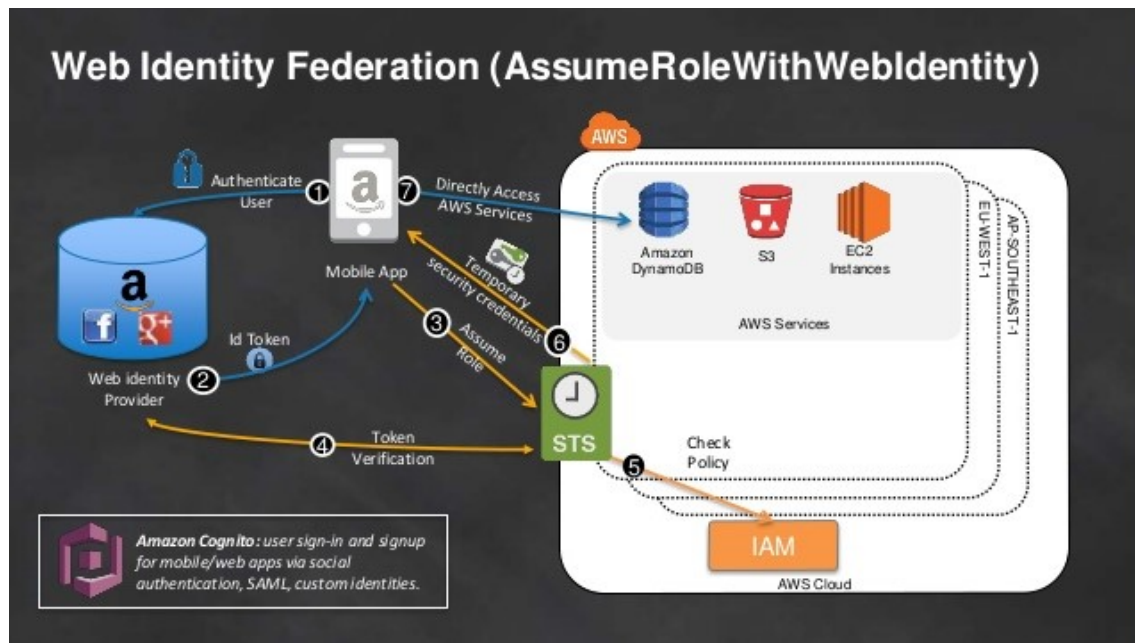
Option B is this is not a feasible configuration.

Option C is correct. In order to use web federated identity to authenticate users create a role with appropriate permission to communicate with DynamoDB, authenticate the user with Web Identity federation ,obtain temporary credentials through the AWS Security Token Service for allowing the application to access the resources.

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 35

UNATTEMPTED

SECURITY

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



Choose 3 options from the below:

- ☐ A. Setting up a federation proxy or identity provider. ✓
- ☐ B. Using AWS Security Token Service to generate temporary tokens. ✓
- ☐ C. Tagging each folder in the bucket.
- ☐ D. Configuring IAM role. ✓
- ☐ E. Setting up a matching IAM user for every user in your corporate directory that needs access to a folder in the bucket.

Explanation :

Answer – A, B, and D

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

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

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

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

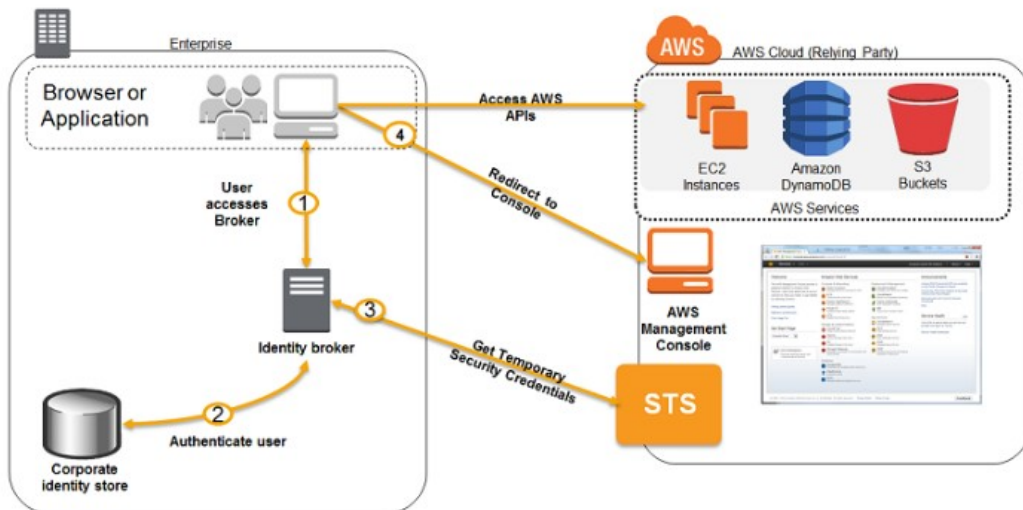
Option C is incorrect because tagging each folder in bucket does not help in this scenario.

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

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

The diagram below showcases how authentication is carried out when having an identity broker. This is an example of a SAML connection , but the same concept holds true for getting access to an AWS resource.





For more information on federated access, please visit the below link
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html
 (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html)

Ask our Experts



QUESTION 36

UNATTEMPTED

SCALABILITY & ELASTICITY

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

Choose 2 answers from the below options:

- ☐ A. Deploy ElasticCache in-memory cache running in each availability zone

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

Explanation :

Answer – A and D

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

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

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

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

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

See more information on Read Replicas and ElastiCache below.

Read Replicas

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

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

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

ElastiCache



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

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

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

Ask our Experts



QUESTION 37

UNATTEMPTED

SCALABILITY & ELASTICITY

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

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

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



- ☐ D. Create an RDS Read Replica for the batch analysis and SQS to send a message to the on-premises system to update the dashboard.

Explanation :

Answer - C

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

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

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

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

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

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

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

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

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

Ask our Experts



QUESTION 38

UNATTEMPTED

SCALABILITY & ELASTICITY

How can you ensure the scalability of an application developed in Java interfacing with DynamoDB to reduce the load on the DynamoDB database?

Choose an answer from the below options:



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

Explanation :

Answer – C

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

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

- Option A is incorrect because adding more databases is not going to reduce the load on existing DynamoDB database. Also, this is not a cost efficient solution.
- Option B is incorrect because increasing the write capacity is an expensive option.
- Option C is CORRECT because it uses SQS to assist in taking over the load from storing the data in DynamoDB, and it is scalable as well as cost efficient.
- Option D is incorrect because MultiAZ configuration is not going to help reduce the load, in fact it will affect the performance as the records in DynamoDB would get replicated in multiple availability zones.

More information on SQS:

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

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

For more information on SQS, please refer to the below URL:

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



Ask our Experts



QUESTION 39

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Which of the following HTTP methods are supported by Amazon CloudFront?

Choose 3 options from the below:

- ☐ A. GET ✓
- ☐ B. POST ✓
- ☐ C. DELETE ✓
- ☐ D. UPDATE

Explanation :

Answer – A, B, and C

Amazon CloudFront supports the following HTTP methods: GET, HEAD, POST, PUT, DELETE, OPTIONS, and PATCH. This means you can improve the performance of dynamic websites that have web forms, comment, and login boxes, “add to cart” buttons or other features that upload data from end users.

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

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

Ask our Experts



What are some of the common types of content that are supported by a web distribution via CloudFront?

Choose 3 options from the below:

- ☐ A. Static content ✓
- ☐ B. Live events ✓
- ☐ C. Multimedia content ✓
- ☐ D. Peer to peer networking

Explanation :

Answer – A, B, and C

You can use web distributions to serve the following content over HTTP or HTTPS:

- Static and dynamic download content, for example, .html, .css, .php, and image files, using HTTP or HTTPS.
- Multimedia content on demand using progressive download and Apple HTTP Live Streaming (HLS).
- A live event, such as a meeting, conference, or concert, in real time. For live streaming, you create the distribution automatically by using an AWS CloudFormation Stack.

Hence, options A, B, and C are CORRECT.

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

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-overview.html>

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

Ask our Experts



A client is using CloudFront with a source which normally serves dynamic content. There is a requirement that as soon the content is changed in the source, it is delivered to the client. Which of the following configuration can be made to fulfill this requirement?

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

Explanation :

Answer - C

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

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

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

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

Option D is incorrect as CloudFront surely serves dynamic content.

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

More information on TTL in CloudFront:

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

Low TTLs

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

For more information on CloudFront dynamic content, please refer to the below URL:
<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html>)

Ask our Experts



QUESTION 42

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You are responsible for a web application that consists of an Elastic Load Balancer (ELB) in front of an Auto Scaling group of Amazon Elastic Compute Cloud (EC2) instances. For a recent deployment of a new version of the application, a new Amazon Machine Image (AMI) was created, and the Auto Scaling group was updated with a new launch configuration that refers to this new AMI. During the deployment, you received complaints from users that the website was responding with errors. All instances passed the ELB health checks. What should you do in order to avoid errors for future deployments? (Choose 2 answers)

- ☐ A. Add an Elastic Load Balancing health check to the Auto Scaling group. Set a short period for the health checks to operate as soon as possible in order to prevent premature registration of the instance to the load balancer.
- ☐ B. Enable EC2 instance CloudWatch alerts to change the launch configuration AMI to the previous one. Gradually terminate instances that are using the new AMI.
- ☐ C. Set the Elastic Load Balancing health check configuration to target a part of the application that fully tests application health and returns an error if the tests fail. ✓

- ☐ D. Create a new launch configuration that refers to the new AMI, and associate it with the group. Double the size of the group, wait for the new instances to become healthy, and reduce back to the original size. If new instances do not become healthy, associate the previous launch configuration. ✓
- ☐ E. Increase the Elastic Load Balancing Unhealthy Threshold to a higher value to prevent an unhealthy instance from going into service behind the load balancer.

Explanation :

Answers - C & D

In this scenario, the ELB health check was passed which implies that the instances were successfully deployed using the new AMIs by the launch configuration and auto scaling group. The deployment was successful, but as the users started using the application, they started receiving the error. So, it implies that the errors are related to the application itself, not the setup.

Option A is incorrect because setting the short period of health check will not be useful in this scenario.

Option B is incorrect because you cannot change the launch configuration based on the CloudWatch alert.

Option C is CORRECT because, the current health check might be just checking if the application/web site is reachable or not. I.e. It may not be currently checking whether the application is fully functioning. If the health check is configured to test the part of the application that fully tests it, it would stop deploying the instances with the faulty application.

Option D is CORRECT because doubling the auto scaling size will give some lead time for instances to become healthy while the AMI with old update gets terminated (kind of Blue/Green Deployment).

Option E is incorrect because increasing the unhealthy threshold will not help in this scenario since it does not prevent unhealthy instances from being deployed.



Ask our Experts



QUESTION 43

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You have deployed a web application targeting a global audience across multiple AWS Regions under the domain name example.com. You decide to use Route53 Latency-Based Routing to serve web requests to the users from the region closest to them. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region.

During a DR test you notice that when you disable all web servers in one of the regions Route53 does not automatically direct all users to the other region. What could be happening? (Choose 2 answers)

- ☐ A. Latency resource record sets cannot be used in combination with weighted resource record sets.
- ☐ B. You did not setup an HTTP health check to one or more of the weighted resource record sets associated with the disabled web servers. ✓
- ☐ C. The value of the weight associated with the latency alias resource record set in the region with the disabled servers is higher than the weight for the other region.
- ☐ D. One of the two working web servers in the other region did not pass its HTTP health check.



- ☐ E. You did not set “Evaluate Target Health” to “Yes” on the latency alias resource record set associated with example.com in the region where you disabled the servers. ✓

Explanation :

Answer - B & E

Option A is incorrect because you can setup weighted record sets as the failover or secondary record set.

Option B is CORRECT because if the HTTP health check is not set with the weighted resource record sets of the disabled web servers, Route 53 will consider them healthy, and will continue to forward the traffic to them. Once the health check is enabled, the DNS queries will get a response indicating that the web servers are disabled, and then the requests would get routed to the other region.

Option C is incorrect because even if the weight is lower for the region with disabled web servers, Route 53 will continue forwarding the requests of the users closest to that region because it will evaluate the latency record set first.

Option D is incorrect because, even if one of the servers fails, the other server will still work and the region should get the traffic.

Option E is CORRECT because if the “Evaluate Target Health” is not set to “Yes” for the region containing the disabled web servers, the Route 53 will consider the health of the record set as healthy and will continue to route the traffic to it.

For more information on How Amazon Route 53 chooses records when Health Checking is configured, please visit the link below:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-how-route-53-chooses-records.html>

(<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-how-route-53-chooses-records.html>)

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html#dns-failover-complex-configs-eth-no>

(<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html#dns-failover-complex-configs-eth-no>)



Ask our Experts



QUESTION 44

UNATTEMPTED

DATA STORAGE

A company is in the evaluation phase of deploying a Redshift cluster. Which of the following types of instances should the company think of deploying for their Redshift cluster during this phase?

Choose an answer from the options given below:

- ☐ A. Reserved instances because they are cost effective
- ☒ B. On-Demand ✓
- ☐ C. Spot Instances because they are the least cost option
- ☐ D. Combination of all 3 types of instances

Explanation :

Answer – B

Option A is incorrect because if the instances are reserved, the company would be in a contract for paying for the instances irrespective whether they utilize all the instances or only some of them.

Option B is CORRECT because in the evaluation phase of your project or when you're developing a proof of concept, on-demand pricing gives you the flexibility to pay as you go, to pay only for what you use, and to stop paying at any time by shutting down or deleting clusters. After you have established the needs of your production environment and begin the implementation phase, you may consider reserving compute nodes by purchasing one or more offerings.

Option C is incorrect because even though the spot instances are cheapest, they involve in risk of shutting down with a very short notice and the price depends upon their current availability. Also, spot instances are recommended only if the application is tolerant of interruptions.



Option D is incorrect because as mentioned above, the reserved instances may not be the best choice since there is no mention of the duration of the evaluation period, and the spot instances cannot be used since there is no mention of the company or its application being tolerant of the interruption risk that are associated with purchasing the spot instances.

For more information on the type of instances to choose for the Redshift cluster please refer to the below URL:

<http://docs.aws.amazon.com/redshift/latest/mgmt/purchase-reserved-node-instance.html> (<http://docs.aws.amazon.com/redshift/latest/mgmt/purchase-reserved-node-instance.html>)

Ask our Experts



QUESTION 45

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

There is a requirement for a high availability and disaster recovery plan for an organization.

Below are the key points for this plan

Once stored successfully, the data should not be lost. This is the key requirement.

Recovery time can be long as this could save on cost.

Which of the following options would be the best one for this corporation, given the concerns that they have outlined to you above?

Choose the correct answer from the below options:

- ☐ **A. Make sure you have RDS set up as an asynchronous Multi-AZ deployment, which automatically provisions and maintains an asynchronous “standby” replica in a different Availability Zone.**



- ☐ B. Set up a number of smaller instances in a different region, which all have Auto Scaling and Elastic Load Balancing enabled. If there is a network outage, then these instances will auto scale up. As long as spot instances are used and the instances are small this should remain a cost effective solution.
- ☐ C. Backup and restoring with S3 should be considered due to the low cost of S3 storage. Backup up frequently and the data can be sent to S3 using either Direct Connect or Storage Gateway, or over the Internet. ✓
- ☐ D. Set up pre-configured servers using Amazon Machine Images. Use an Elastic IP and Route 53 to quickly switch over to your new infrastructure if there are any problems when you run your health checks.

Explanation :

Answer - C

Option A is incorrect because it can help in maintaining data, but is not low on cost and is a high-cost option since you need to maintain a multi-AZ environment. Hence we need to count this option out.

Option B is incorrect because it does not talk about data loss avoidance and is more of network avoidance.

Option C is CORRECT because S3 provides durable, highly available, low cost and more secure storage solution.

Option D is incorrect because it talks about AMI's but not about the underlying data on EBS storage which will need to be backed up.

More information about Amazon S3:

Amazon S3 is storage for the Internet. It's a simple storage service that offers software developers a highly-scalable, reliable, and low-latency data storage infrastructure at very low costs.

For more information on S3 please refer to the below link

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

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

Ask our Experts



Your company would be assigning an auditor that would view all the logs of your AWS environment.

Which of the below option would be the best solution for the auditor to ensure that they can view the logs in the AWS environment?

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

Explanation :

Answer – D

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

Option B is incorrect because sending the logs via email is not a good architecture.

Option C is incorrect because granting the auditor access to AWS resources is not AWS's responsibility. It is the AWS user or account owner's responsibility.

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

More information on AWS CloudTrail:

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a

history of AWS API calls for your account, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.

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

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

Ask our Experts



QUESTION 47

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

A company has setup a Direct Connect connection between their on-premise location and their AWS VPC. They want to setup redundancy in case the Direct Connect connection fails. What can they do in this regard?

Choose 2 options from the below:

- ☐ A. Setup another Direct Connect connection. ✓
- ☐ B. Setup an IPSec VPN Connection. ✓
- ☐ C. Setup S3 connection.
- ☐ D. Setup a connection via EC2 instances.

Explanation :

Answer – A and B

Option A and B are CORRECT because with A, you can have a redundant Direct Connect setup as a backup if the main Direct Connect connection fails (even though it is an expensive solution, it will work), and with B, VPN is an alternate way for the connection between AWS and on-premises infrastructure (even though it is a slower connectivity, it will work).



More information on Direct Connect:

If you have established a second AWS Direct Connect connection, traffic will failover to the second link automatically. We recommend enabling Bidirectional Forwarding Detection (BFD) when configuring your connections to ensure fast detection and failover. If you have configured a backup IPsec VPN connection instead, all VPC traffic will failover to the VPN connection automatically. Traffic to/from public resources such as Amazon S3 will be routed over the Internet. If you do not have a backup AWS Direct Connect link or an IPsec VPN link, then Amazon VPC traffic will be dropped in the event of a failure. Traffic to/from public resources will be routed over the Internet.

For more information on Direct Connect FAQ's, please visit the below URL:

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

Ask our Experts



QUESTION 48

UNATTEMPTED

COSTING

Your company is storing millions of sensitive transactions across thousands of 100-GB files that must be encrypted in-transit and at-rest. Analysts concurrently depend on subsets of files, which can consume up to 5 TB of space, to generate simulations that can be used to steer business decisions. You are required to design an AWS solution that can cost effectively accommodate the long-term storage and in-flight subsets of data. Which one would you choose?

- ☐ A. Use Amazon Simple Storage Service (S3) with server-side encryption, and run simulations on subsets in ephemeral drives on Amazon EC2.
- ☐ B. Use Amazon S3 with server-side encryption, and run simulations on subsets in-memory on Amazon EC2.
- ☐ C. Use HDFS on Amazon EMR, and run simulations on subsets in ephemeral drives on Amazon EC2.



- ☐ D. Use HDFS on Amazon Elastic MapReduce (EMR), and run simulations on subsets in-memory on Amazon Elastic Compute Cloud (EC2). ✓
- ☐ E. Store the full data set in encrypted Amazon Elastic Block Store (EBS) volumes, and regularly capture snapshots that can be cloned to EC2 workstations.

Explanation :

Answer - D

The main considerations of this scenario are: (1) the solution must be cost-effective, (2) provide long-term storage, and (3) encrypt in-transit as well as at-rest data.

Option A is incorrect because, (a) server side encryption does not apply to in-transit data, and (b) ephemeral volumes are not encrypted at rest.

Option B is incorrect because, it does not support encryption of in-transit data.

Option C is incorrect because, ephemeral drive is not a long term storage.

Option D is CORRECT because, (a) EMR supports both in-transit and at-rest data encryption, and (b) HDFS provides the long term storage.

Option E is incorrect because, this is not a cost-effective solution.

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

- <https://aws.amazon.com/blogs/aws/new-at-rest-and-in-transit-encryption-for-amazon-emr/> (<https://aws.amazon.com/blogs/aws/new-at-rest-and-in-transit-encryption-for-amazon-emr/>)
- <https://d0.awsstatic.com/whitepapers/aws-amazon-emr-best-practices.pdf> (<https://d0.awsstatic.com/whitepapers/aws-amazon-emr-best-practices.pdf>)

Ask our Experts



As an IT administrator, you have been tasked to ensure that SQL injection attacks are kept at bay. You currently maintain a set of applications hosted on AWS which consists of a fleet of EC2 instances. Which of the below approach provides a cost-effective scalable mitigation to this kind of attack?

- ☐ **A.** Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC. Then they would establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF) and then pass the traffic through the DirectConnect connection into their application running in their VPC.
- ☐ **B.** Add previously identified host file source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
- ☐ **C.** Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group. ✓
- ☐ **D.** Remove all but TLS 1 & 2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Explanation :

Answer – C

In such scenarios where you are designing a solution to prevent the DDoS attack, always think of using Web Application Firewall (WAF).

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

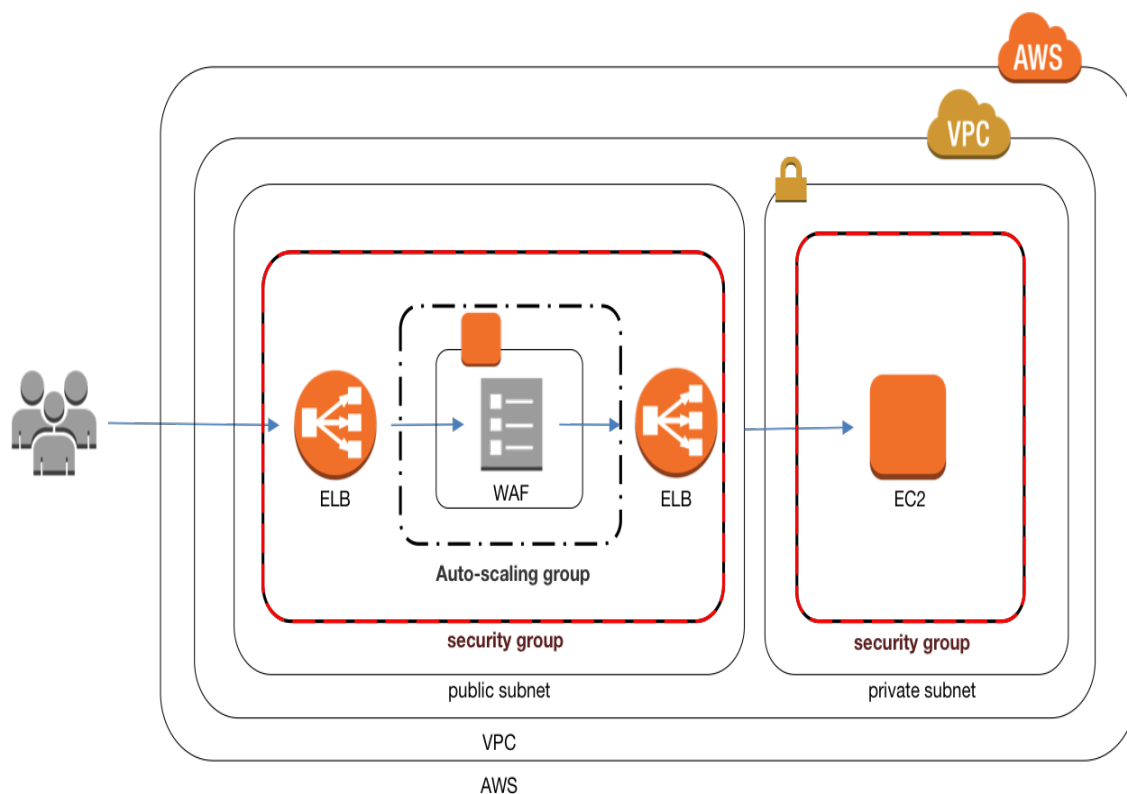
Option A is incorrect because, although this option could work, the setup is very complex



and it is not a cost effective solution.

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

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



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

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

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



Ask our Experts



QUESTION 50

UNATTEMPTED

DEPLOYMENT MANAGEMENT

As an IT administrator, you have been requested to manage the CloudFormation stacks for a set of developers in your company. A set of web and database developers will be working on the application. How would you design the CloudFormation stacks in the best way possible?

- ☐ A. CloudFormation is not the right fit, use OpsWork instead.
- ☐ B. Create one stack for the web and database developers.
- ☒ C. Create separate stacks for the web and database developers. ✓
- ☐ D. Define separate EC2 instances since defining CloudFormation can get cumbersome.

Explanation :

Answer – C

Option A is incorrect because CloudFormation is best for creating and maintaining all the infrastructure resources in the cloud environment.

Option B is incorrect because as your stack grows in scale and broadens in scope, managing a single stack can be cumbersome and time consuming. Also, coordinating and communicating updates can become difficult.

Option C is CORRECT because (a) having multiple (or sub) stacks is easier to maintain, (b) there is a clear separation of ownership and concerns, (c) better chances of you staying within the limit for 'Template body size' which happens to be 460,800 bytes, and (d) you can reuse common template patterns. See "More information..." section for more details.

Option D is incorrect because you can provision and maintain the infrastructure if the CloudFormation templates are created correctly.

More information on CloudFormation Best Practices:

The following use case scenario is given in the AWS documentation to support the answer:



For example, imagine a team of developers and engineers who own a website that is hosted on autoscaling instances behind a load balancer. Because the website has its own lifecycle and is maintained by the website team, you can create a stack for the website and its resources. Now imagine that the website also uses back-end databases, where the databases are in a separate stack that is owned and maintained by database administrators. Whenever the website team or database team needs to update their resources, they can do so without affecting each other's stack. If all resources were in a single stack, coordinating and communicating updates can be difficult.

For more information on CloudFormation best practices, please visit the below URL
<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html>
(<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html>)

Ask our Experts



QUESTION 51

UNATTEMPTED

DATA STORAGE

You need a persistent and durable storage to trace call activity of an IVR (Interactive Voice Response) system. Call duration is mostly in the 2-3 minutes time-frame. Each traced call can be either active or terminated. An external application needs to know each minute the list of currently active calls, which are usually a few calls/second. Put once per month there is a periodic peak up to 1000 calls/second for a few hours. The system is open 24/7 and any downtime should be avoided. Historical data is periodically archived to files. Cost saving is a priority for this project. What database implementation would better fit this scenario, keeping the costs as low as possible?

- ☐ A. Use RDS Multi-AZ with two tables, one for "Active calls" and one for "Terminated calls". In this way, the "Active calls" table is always small and effective to access.



- ☐ B. Use DynamoDB with a "Calls" table and a Global Secondary Index on a "IsActive" attribute that is present for active calls only. In this way, the Global Secondary index is sparse and more effective. ✓
- ☐ C. Use DynamoDB with a "Calls" table and a Global secondary Index on a "State" attribute that can equal to "active" or "terminated". In this way, the Global Secondary index can be used for all Items in the table.
- ☐ D. Use RDS Multi-AZ with a "Calls" table and an indexed "State" field that can be equal to "Active" or "Terminated". In this way, the SQL query is optimized by the use of the Index.

Explanation :

Answer - B

The important consideration in this scenario is that the application needs to know each minute the list of **currently active calls**.i.e. The application does not need to know about the terminated calls. The idea behind sparse indexes is that only items with IsActive = "Y" will be in the index, so require less storage and processing than your main table.

Option A is incorrect because keeping the information about the terminated calls is not needed. So, having a table for that would not be an optimized or cost-effective solution.

Option B is CORRECT because (a) it keeps the information about active calls via "IsActive" attribute only for the active calls, (b) it has a GSI which is optimally utilized for active calls only, keeping the use of it to minimum; hence, saving the cost, and (c) in this scenario, setting up DynamoDB is more cost saving solution than RDS.

Option C is incorrect because (a) keeping the information about the terminated calls is not needed, and (b) setting a GSI on all items will not be an optimized and cost-effective solution.

Option D is incorrect because (a) keeping the information about the terminated calls is not needed, and (b) in this scenario, setting up RDS is more costly solution than DynamoDB.

More information on Best Practices for DynamoDB:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html#GuidelinesForGSI.SparseIndexes>

(<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html#GuidelinesForGSI.SparseIndexes>)



Ask our Experts



QUESTION 52

UNATTEMPTED

NETWORK DESIGN

A customer is hosting their company website on a cluster of web servers that are behind a public-facing load balancer. The customer also uses Amazon Route 53 to manage their public DNS. How should the customer configure the DNS zone apex record to point to the load balancer?

- ☐ A. Create an A record pointing to the IP address of the load balancer.
- ☐ B. Create a CNAME record pointing to the load balancer DNS name.
- ☐ C. Create a CNAME record aliased to the load balancer DNS name.
- ☒ D. Create an A record aliased to the load balancer DNS name. ✓

Explanation :

Answer – D

Option A is incorrect because it suggests to create A record pointing to the IP address of the ELB; but, ELB's don't have predefined IP addresses.

Option B and C are incorrect because you should preferably create ALIAS record rather than CNAME record. See the "More information..." section for more details.

Option D is CORRECT because it creates an A record, but instead of pointing to an IP address, it ALIASES it to the DNS of the ELB.

More information on ALIAS Record:

Alias resource record sets are virtual records that work like CNAME records. But they differ from CNAME records in that they are not visible to resolvers. Resolvers only see the A record and the resulting IP address of the target record. As such, unlike CNAME records, alias resource record sets are available to configure a zone apex (also known as a root domain or naked domain) in a dynamic environment.



For more information on the zone apex, please refer to the link below:

<http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html> (<http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html>)

For more information on choosing between ALIAS and Non-ALIAS records, please refer to the link below:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html?console_help=true

(https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html?console_help=true)

Ask our Experts



QUESTION 53

UNATTEMPTED

DEPLOYMENT MANAGEMENT

By default, when an EBS volume is attached to a Windows instance, it may show up as any drive letter on the instance. For which services can you use to change the settings of the drive letters of the EBS volumes per your specifications?

- ☐ A. EBSService
- ☐ B. AMIService
- ☒ C. EC2Config Service ✓
- ☐ D. EC2-AMIService

Explanation :

Answer – C

Windows AMIs include an optional service called the EC2Config service (EC2Config.exe). EC2Config starts when the instance boots and performs tasks during startup and each time you stop or start the instance. EC2Config can also perform tasks on demand. Some of these



tasks are automatically enabled, while others must be enabled manually. Although optional, this service provides access to advanced features that aren't otherwise available. This service runs in the LocalSystem account.

For more information on EC2 Config service, please visit the link
http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/UsingConfig_WinAMI.html
(http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/UsingConfig_WinAMI.html)

Ask our Experts



QUESTION 54

UNATTEMPTED

CLOUD MIGRATION & HYBRID ARCHITECTURE

You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet as well as from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link. How would you design routing to meet the above requirements?

- ☐ A. Configure a single routing table with a default route via the Internet gateway. Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.
- ☐ B. Configure a single routing table with a default route via the Internet gateway. Propagate specific routes for the on-premises networks via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets. ✓
- ☐ C. Configure a single routing table with two default routes: one to the Internet via an Internet gateway the other to the on-premises network via the VPN gateway. Use this routing table across all subnets in your VPC.
- ☐ D. Configure two routing tables: one that has a default route via the Internet gateway, and another that has a default route via the VPN gateway. Associate both routing tables with each VPC subnet. ^

Explanation :

Answer - B

Option A and C are incorrect because, two default routes cannot be configured in the route table.

Option B is CORRECT because with this setup, the route via the BGP(which is specific) will be preferred over the one via Internet gateway (default).

Option D is incorrect because the subnet in which the instances are placed, can have a single routing table associated with them.

More information on Route Tables and VPN Route Priority::

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-priority

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

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-route-priority

(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-route-priority)

Ask our Experts



QUESTION 55

UNATTEMPTED

SCALABILITY & ELASTICITY

Which of the following can be done by Auto scaling?

Choose 2 answers from the options given below:

- ☐ A. Start up EC2 instances when CPU utilization is above threshold. ✓
- ☐ B. Release EC2 instances when CPU utilization is below threshold. ✓
- ☐ C. Increase the instance size when utilization is above threshold.



☐ **D. Decrease the instance size when utilization is below threshold.**

Explanation :

Answer - A and B

Option A and B are CORRECT because AutoScaling can start or terminate instances based on CPU utilization.

Option C and D are incorrect because AutoScaling cannot increase or decrease the instance size based on CPU utilization. It will launch the instances based on the launch configuration.

As per the AWS documentation, below is what can be done with Auto Scaling. You can only scale horizontally and not vertically.

- Scale-out Amazon EC2 instances seamlessly and automatically when demand increases.
- Shed unneeded Amazon EC2 instances automatically and save money when demand subsides.
- Scale dynamically based on your Amazon CloudWatch metrics, or predictably according to a schedule that you define.
- Replace unhealthy or unreachable instances to maintain the higher availability of your applications.
- Receive notifications via Amazon Simple Notification Service (Amazon SNS) to be alerted when you use Amazon CloudWatch alarms to initiate Auto Scaling actions, or when Auto Scaling completes an action.
- Run On-Demand or Spot Instances, including those inside your virtual private cloud (VPC) or high performance computing (HPC) clusters.
- If you're signed up for the Amazon EC2 service, you're already registered to use Auto Scaling and can begin using the feature via the API or command line interface.

For more information on Auto scaling please visit the link

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



Ask our Experts



QUESTION 56

UNATTEMPTED

NETWORK DESIGN

There is a requirement to create EMR jobs that shift through all of the web server logs and error logs to pull statistics on click stream and errors based off of client IP address. Given the requirements what would be the best method for collecting the log data and analyzing it automatically?

Choose the correct answer from the below options:

- ☐ A. If the application is using HTTP, you need to configure proxy protocol to pass the client IP address in a new HTTP header. If the application is using TCP, modify the application code to pull the client IP into the x-forward-for header so the web servers can parse it.
- ☐ B. Configure ELB access logs then create a Data Pipeline job which imports the logs from an S3 bucket into EMR for analyzing and output the EMR data into a new S3 bucket.
- ☐ C. If the application is using TCP, configure proxy protocol to pass the client IP address in a new TCP header. If the application is using, HTTP modify the application code to pull the client IP into the x-forward-for header so the web servers can parse it. ✓
- ☐ D. Configure ELB error logs then create a Data Pipeline job which imports the logs from an S3 bucket into EMR for analyzing and outputs the EMR data into a new S3 bucket.

Explanation :

Answer – C

Option A is incorrect because (a) if the protocol is TCP, you can use proxy protocol to pass the client IP address in a new TCP header, and (b) x-forward-for header is to be used only if the protocol is HTTP. ✓

Option B is incorrect because it does not specify how error logs would be configured and analyzed.

Option C is CORRECT because (a) the requirement is to scan both the web server logs and error logs, and (b) the webserver being behind the ELB would not receive the client IP address and would need proxy protocol for TCP or x-forward-for header for HTTP traffic.

Option D is incorrect because it does not specify how access logs would be configured and analyzed.

For more information on HTTP Headers and Classic ELB, please refer to the links below:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html>

(<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html>)

Ask our Experts



QUESTION 57

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

Which of the following benefits does adding Multi-AZ deployment in RDS provide?

Choose 2 answers from the options given below:

- ☐ A. Multi-AZ deployed database can tolerate an Availability Zone failure. ✓
- ☐ B. Decrease latencies if app servers accessing database are in multiple Availability zones.
- ☐ C. Make database access times faster for all app servers.
- ☐ D. Make database more available during maintenance tasks. ✓

Explanation :

Answer - A and D



Option A is CORRECT because in Multi-AZ deployment, if an availability zone (AZ) goes down, the automatic failover occurs and the DB instance CNAME gets pointed to the synchronously updated secondary instance in another AZ.

Option B is incorrect because Multi-AZ deployment does not affect the latency of the application's DB access.

Option C is incorrect because DB access time does not get affected by Multi-AZ deployment.

Option D is CORRECT because during the maintenance tasks, the DB instance CNAME can point to the secondary instance in another AZ to carry out the DB tasks.

Some of the advantages of Multi-AZ rds deployments are given below

- If an Availability Zone failure or DB Instance failure occurs, your availability impact is limited to the time automatic failover takes to complete.
- The availability benefits of Multi-AZ deployments also extend to planned maintenance and backups. In the case of system upgrades like OS patching or DB Instance scaling, these operations are applied first on the standby, prior to the automatic failover. As a result, your availability impact is, again, only the time required for automatic failover to complete.
- If a storage volume on your primary fails in a Multi-AZ deployment, Amazon RDS automatically initiates a failover to the up-to-date standby.

For more information on Multi-AZ rds deployments please visit the link

<https://aws.amazon.com/rds/details/multi-az/> (<https://aws.amazon.com/rds/details/multi-az/>)

Ask our Experts



QUESTION 58

UNATTEMPTED

DEPLOYMENT MANAGEMENT

What of the following is true about the features Lambda@Edge in AWS?

Choose an answer from the options given below:

- ☐ A. It is used specifically for the Edge based programming language.



- ☐ B. It is used for running Lambda functions at edge locations defined by S3.
- ☐ C. It is used for running Lambda functions at edge locations used by CloudFront. ✓
- ☐ D. It can support any type of programming language.

Explanation :

Answer – C

Option A is incorrect as it is not used for Edge based programming.

Option B is incorrect because edge locations are part of CloudFront setup, not S3.

Option C is CORRECT because Lambda@Edge allows you to run Lambda functions at the AWS edge locations in response to CloudFront events. Without Lambda@Edge, customized processing requires requests to be forwarded back to compute resources at the centralized servers. This slows down the user experience.

Option D is incorrect because Lambda@Edge supports only Node.js, which is a server-side JavaScript framework.

For more information on Lambda@Edge please visit the link:

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/what-is-lambda-at-edge.html>

(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/what-is-lambda-at-edge.html>)

Ask our Experts



QUESTION 59

UNATTEMPTED

SCALABILITY & ELASTICITY

Which of the following reports in CloudFront can help find out the most popular requested objects at an edge location?

Choose an answer from the options given below

- ☐ A. Cache Statistics



- ☐ B. Most requested
- ☐ C. Most Referred
- ☐ D. Top Referrers
- ☒ E. Popular Objects ✓

Explanation :

Answer – E

Amazon CloudFront Popular Objects Report

Track Your Most Popular Objects

The Popular Objects Report shows request count, cache hit and cache miss counts, as well as error rates for the 50 most popular objects during the specified period. This helps you understand which content is most popular among your viewers, or identify any issues (such as high error rates) with your most requested objects.

There are no additional charges for the Popular Objects Report. To view the reports, simply navigate to the AWS Management Console, navigate to Amazon CloudFront and select Popular Objects under the Reports and Analytics link in the navigation pane.

Rank	Object Key	Size	Type	Status	Request Count	Hit Count	Miss Count	Error Count
1	/static/images/logo.png	10	20	200	100	100	0	0
2	/static/images/logo.png	10	20	200	100	100	0	0
3	/static/images/logo.png	10	20	200	100	100	0	0
4	/static/images/logo.png	10	20	200	100	100	0	0
5	/static/images/logo.png	10	20	200	100	100	0	0
6	/static/images/logo.png	10	20	200	100	100	0	0
7	/static/images/logo.png	10	20	200	100	100	0	0
8	/static/images/logo.png	10	20	200	100	100	0	0
9	/static/images/logo.png	10	20	200	100	100	0	0
10	/static/images/logo.png	10	20	200	100	100	0	0



CloudFront Popular Objects Report

The Amazon CloudFront console can display a list of the 50 most popular objects for a distribution during a specified date range in the previous 60 days.

Data for the Popular Objects report is drawn from the same source as CloudFront access logs. To get an accurate count of the top 50 objects, CloudFront counts the requests for all of your objects in 10-minute intervals beginning at midnight and keeps a running total of the top 150 objects for the next 24 hours. (CloudFront also retains daily totals for the top 150 objects for 60 days.) Near the bottom of the list, objects constantly rise onto or drop off of the list, so the totals for those objects are approximations. The fifty objects at the top of the list of 150 objects may rise and fall within the list, but they rarely drop off of the list altogether, so the totals for those objects typically are more reliable.

For more information on the popular objects report please visit the link:

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

Ask our Experts



QUESTION 60

UNATTEMPTED

SCALABILITY & ELASTICITY

Which of the following media servers can be used for live media streaming with CloudFront?

Choose 3 options from the below:

- ☐ A. Adobe Media Server ✓
- ☐ B. IIS Media services ✓
- ☐ C. Atlassian Media Servers
- ☐ D. Wowza streaming engine ✓



Explanation :

Answer: A, B, and D

You can use following live media servers for streaming media via CloudFront:

- Adobe Flash Media Server
- Windows IIS Media Services
- Wowza Streaming Engine

Hence, options A, B, and D are CORRECT.

For more information please refer to the links below:

<https://aws.amazon.com/blogs/aws/live-streaming-with-amazon-cloudfront-and-adobe-flash-media-server/> (<https://aws.amazon.com/blogs/aws/live-streaming-with-amazon-cloudfront-and-adobe-flash-media-server/>)

<https://aws.amazon.com/blogs/aws/smooth-streaming-with-cloudfront-and-windows-media-services/> (<https://aws.amazon.com/blogs/aws/smooth-streaming-with-cloudfront-and-windows-media-services/>)

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

Ask our Experts



QUESTION 61

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You are moving an existing traditional system to AWS. During migration, you discover that the master server is the single point of failure. Having examined the implementation of the master server you realize that there is not enough time during migration to re-engineer it to be highly available. You also discover that it stores its state in local MySQL database.



In order to minimize downtime, you select RDS to replace the local database and configure the master to use it. What steps would best allow you to create a self-healing architecture?

- ☐ **A. Migrate the local database into Multi-AZ database. Place the master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks. ✓**
- ☐ **B. Migrate the local database into Multi-AZ database. Place the master node into a Cross Zone ELB with a minimum of one and maximum of one with health checks.**
- ☐ **C. Replicate the local database into a RDS Read Replica. Place the master node into a Cross Zone ELB with a minimum of one and maximum of one with health checks.**
- ☐ **D. Replicate the local database into a RDS Read Replica. Place the master node into a multi-AZ auto-scaling group with a minimum of one and maximum of one with health checks.**

Explanation :

Answer - A

Option A is CORRECT because (i) for database, Multi-AZ architecture provides high availability and can meet shortest of RTO and RPO requirements in case of failures, since it uses synchronous replication and maintains standby instance which gets promoted to primary, and (ii) for master server, it uses auto scaling which ensures that at least one server is always running.

Option B is incorrect because ELB cannot ensure the minimum or maximum number of instances running.

Option C is incorrect because (i) read replicas do not provide high availability, and (ii) ELB cannot ensure the minimum or maximum number of instances running.

Option D is incorrect because read replicas do not provide high availability.

More information on Multi-AZ RDS architecture:

Multi-AZ is used for highly available architecture. If a failover happens, the secondary DB which is a synchronous replica will have the data, and it's just the CNAME which changes. For Read replica, it's primarily used for distributing workloads.



For more information on Multi-AZ RDS, please refer to the below link

<https://aws.amazon.com/rds/details/multi-az/> (<https://aws.amazon.com/rds/details/multi-az/>)

Ask our Experts



QUESTION 62

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You have created an OpsWorks stack to create EC2 instances along with an ELB. You have now been asked to change the region in which the EC2 instances will be registered. Can you change the region value in the OpsWorks stack?

- ☐ A. Yes
- ☒ B. No ✓

Explanation :

Answer - B

After you create a layer, some properties (such as AWS region) are immutable, but you can change most of the layer configuration at any time.

For more information on working with OpsWorks layers, please refer to the below link

- <http://docs.aws.amazon.com/opsworks/latest/userguide/workinglayers-basics-edit.html> (<http://docs.aws.amazon.com/opsworks/latest/userguide/workinglayers-basics-edit.html>)

Ask our Experts



QUESTION 63

UNATTEMPTED

DEPLOYMENT MANAGEMENT

What are the steps that get carried out by OpsWork when you attach a load balancer to a layer in OpsWork?

Choose 3 options from the below:

- ☐ A. Terminates the EC2 Instances.
- ☐ B. Deregisters any currently registered instances. ✓
- ☐ C. Automatically registers the layer's instance's when they come online and deregisters instances when they leave the online state, including load-based and time-based instances. ✓
- ☐ D. Automatically activates and deactivates the instances' Availability Zones. ✓

Explanation :

Answer– B, C, and D

For the exam remember that, after you attach a load balancer to a layer, AWS OpsWorks Stacks does the following:

- Deregisters any currently registered instances.
- Automatically registers the layer's instance's when they come online and deregisters instances when they leave the online state, including load-based and time-based instances.
- Automatically activates and deactivates the instances' Availability Zones.

Hence, options B, C, and D are CORRECT.

For more information on working with Opswork layer ELB's, please refer to the below link

<http://docs.aws.amazon.com/opsworks/latest/userguide/layers-elb.html>
(<http://docs.aws.amazon.com/opsworks/latest/userguide/layers-elb.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



QUESTION 65

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)





QUESTION 66

UNATTEMPTED

NETWORK DESIGN

A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnet. Which of the below-mentioned options cannot be the correct IP address (private IP) assigned to an instance in the public or private subnet?

- ☒ A. 20.0.0.255 ✓
- ☐ B. 20.0.0.132
- ☐ C. 20.0.0.122
- ☐ D. 20.0.0.55

Explanation :

Answer – A

In Amazon VPC, the first four IP addresses and the last IP address in each subnet CIDR block are not available for the user to assign to an instance. For example, in this VPC, the following five IP addresses are reserved:

- 20.0.0.0: Network address.
- 20.0.0.1: Reserved by AWS for the VPC router.
- 20.0.0.2: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two.
- 20.0.0.3: Reserved by AWS for future use.
- 20.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

For more information on IP Reservation, please visit the link

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



Ask our Experts



QUESTION 67

UNATTEMPTED

DEPLOYMENT MANAGEMENT

You've been working on a CloudFront whole site CDN. After configuring the whole site CDN with a custom CNAME and supported HTTPS custom domain (i.e., <https://domain.com>) you open domain.com and are receiving the following error:

"CloudFront wasn't able to connect to the origin."

What might be the most likely cause of this error and how would you fix it?

Choose the correct answer from the below options:

- ☐ A. The HTTPS certificate is expired or missing a third party signer. To resolve this purchase and add a new SSL certificate.
- ☐ B. HTTPS isn't configured on the CloudFront distribution but is configured on the CloudFront origin.
- ☐ C. The origin on the CloudFront distribution is the wrong origin.
- ☐ D. The Origin Protocol Policy is set to Match Viewer and HTTPS isn't configured on the origin. ✓

Explanation :

Answer – D

Option A,B, and C are all incorrect because in these scenarios, the CloudFront returns HTTP status code 502 (Bad Gateway).

Option D is CORRECT because this error occurs when the Origin Protocol Policy is set to Match Viewer but HTTPS isn't configured on the origin.

For more information on CloudFront CDN please see the below link



<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html>
(<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html>)
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/http-502-bad-gateway.html#ssl-certificate-expired>
(<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/http-502-bad-gateway.html#ssl-certificate-expired>)

Ask our Experts



QUESTION 68

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A user is using a small MySQL RDS DB. The user is experiencing high latency due to the Multi-AZ feature. Which of the below-mentioned options may not help the user in this situation?

- ☐ A. Schedule the automated back up in non-working hours
- ☐ B. Use a large or higher size instance
- ☐ C. Use Provisioned IOPS storage
- ☐ D. Take a snapshot from standby Replica ✓

Explanation :

Answer – D

- Option A is incorrect because scheduling the automated backups in non-working hours will reduce the load on the DB instance and will help reducing the latency.
- Option B is incorrect because using a larger instance would help processing the queries and carry out load efficiently, thus reducing the overall latency.
- Option C is incorrect because using the provisioned IOPS, the users would get high throughput from the DB instance.



- Option D is CORRECT because taking the snapshots from the read replica is not going to affect the RDS instance. Hence, the users will keep experiencing the high latency as they currently are.

More information on Multi-AZ deployment:

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. As per AWS, the below are the best practices for multiAZ.

For production workloads, we recommend you use Provisioned IOPS and DB instance classes (m1.large and larger) that are optimized for Provisioned IOPS for fast, consistent performance. Hence option B and C are valid.

Also if backups are scheduled during working hours, then I/O can be suspended and increase the latency of the DB, hence it is better to schedule outside of office hours.

For more information on Multi-AZ RDS, please visit the link:

- <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>
(<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>)

Ask our Experts



QUESTION 69

UNATTEMPTED

NETWORK DESIGN

A user has created a public subnet with VPC and launched an EC2 instance within it. The user is trying to delete the subnet. What will happen in this scenario?

- ☐ A. It will delete the subnet and make the EC2 instance as a part of the default subnet.
- ☐ B. It will not allow the user to delete the subnet until the instances are terminated. ✓
- ☐ C. It will delete the subnet as well as terminate the instances.



- ☐ D. The subnet can never be deleted independently, but the user has to delete the VPC first.

Explanation :

Answer – B

In AWS, when you try to delete a subnet which has instances it will not allow to delete it. The below error message will be shown when u try to delete a subnet with instances. Hence, option B is the CORRECT answer.

Delete Subnet ✕

The following subnets contain one or more instances or network interfaces. You cannot delete these subnets until those instances have been terminated, and the network interfaces have been deleted.

- subnet-dfd2a5f2 | Default

[Click here to view your instances.](#)
[Click here to view your network interfaces.](#)

Cancel Yes, Delete

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

Ask our Experts



QUESTION 70

UNATTEMPTED

NETWORK DESIGN

A user has created a VPC with public and private subnets using the VPC wizard by selecting NAT Instance for internet Access. The user has not launched any instance manually and is trying to delete the VPC. What will happen in this scenario?

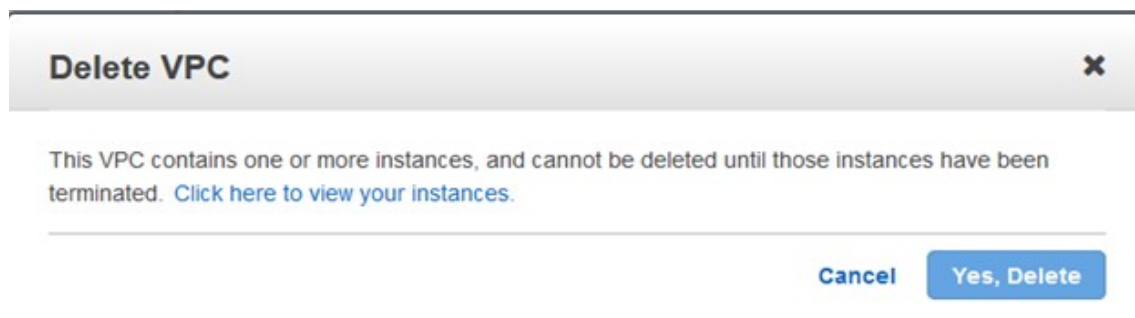


- ☐ A. It will not allow to delete the VPC as it has subnets with route tables.
- ☐ B. It will not allow to delete the VPC since it has a running route instance.
- ☐ C. It will terminate the VPC along with all the instances launched by the wizard.
- ☐ D. It will not allow to delete the VPC since it has a running NAT instance. ✓

Explanation :

Answer – D

Since the VPC will contain a NAT instance because of the private/public subnet combination, when you try to delete the VPC you will get the below error message. Hence, option D is CORRECT.



For more information on VPC and subnets please visit the link

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

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

Ask our Experts



QUESTION 71

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

A user is planning to set up-the Multi-AZ feature of RDS. Which of the below-mentioned conditions won't take advantage of the Multi-AZ feature? ✓

- ☐ A. Availability zone outage
- ☐ B. A manual failover of the DB instance using Reboot with failover option
- ☒ C. Region outage ✓
- ☐ D. When the user changes the DB instance's server type

Explanation :

Answer – C

Amazon RDS handles failovers automatically so you can resume database operations as quickly as possible without administrative intervention. The primary DB instance switches over automatically to the standby replica if any of the following conditions occur:

- An Availability Zone outage
- The primary DB instance fails
- The DB instance's server type is changed
- The operating system of the DB instance is undergoing software patching
- A manual failover of the DB instance was initiated using Reboot with failover

Hence, option A, B and D are incorrect. Option C is CORRECT because if there is a region-wide failure, the Multi-AZ feature may not work.

For more information on multiAZ RDS please visit the link:

<https://aws.amazon.com/rds/details/multi-az/> (<https://aws.amazon.com/rds/details/multi-az/>)

Ask our Experts



A user has created a VPC with public and private subnets using the VPC wizard. Which of the below-mentioned statements is not true in this scenario?

- ☐ A. The VPC will create a routing instance and attach it with a public subnet.
✓
- ☐ B. The VPC will create two subnets.
- ☐ C. The VPC will create one internet gateway and attach it to VPC.
- ☐ D. The VPC will launch one NAT Gateway with an elastic IP.

Explanation :

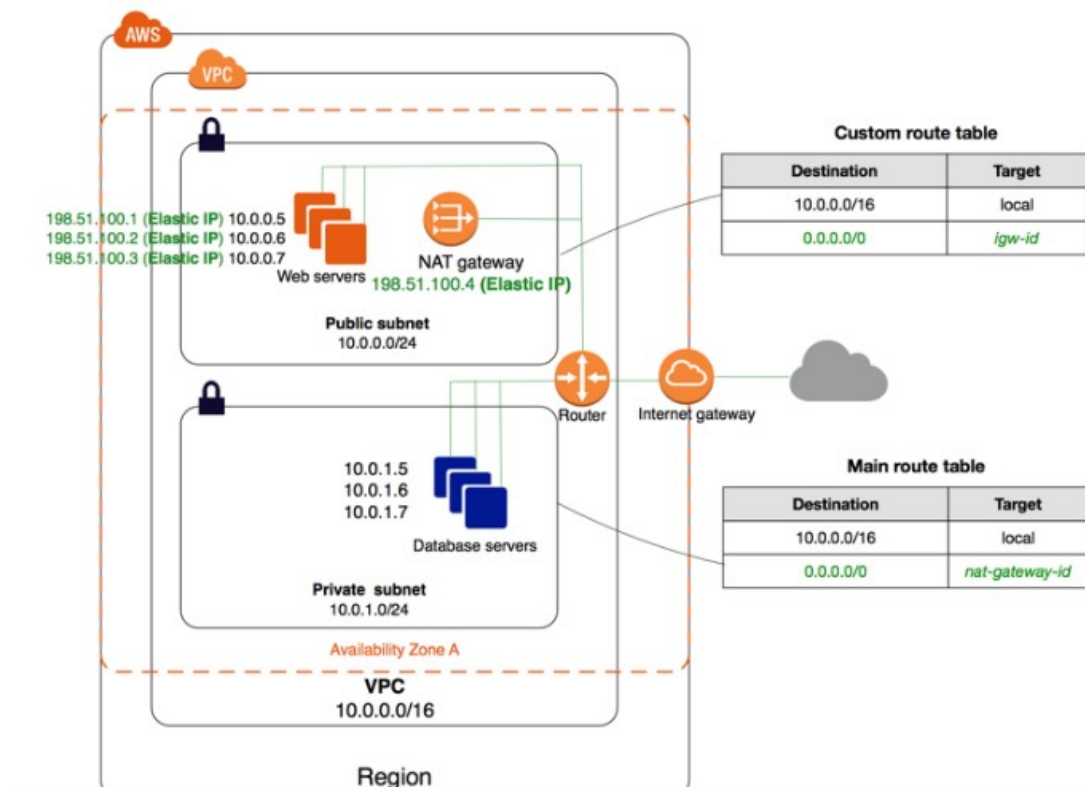
Answer – A

Option A is CORRECT because VPC wizard does not create any routing instance in the public subnet.

Below is the general diagram of what is created when you have a private and public subnet used when using the VPC wizard. So you will get the below options

- 2 subnets – one private and one public
- One NAT Gateway to route traffic from the public to private subnet
- One internet gateway attached to the VPC.





For more information on VPC and subnets, please visit the URL:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html
 (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

Ask our Experts



QUESTION 73

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Which of the following types of servers would this CloudFormation template be most appropriate for? Choose a correct answer from the below options:

{

"AWSTemplateFormatVersion": "2010-09-09",

"Description": "My CloudFormation Template",



```
"Resources": {  
  "MyInstance": {  
    "Type": "AWS::EC2::Instance",  
    "Properties": {  
      "InstanceType": "t2.micro",  
      "ImageId": "ami-030f4133",  
      "NetworkInterfaces": [{  
        "AssociatePublicIpAddress": "true",  
        "DeviceIndex": "0",  
        "DeleteOnTermination": "true",  
        "SubnetId": "subnet-0c2c0855",  
        "GroupSet": ["sg-53a4e434"]  
      }  
    ]  
  }  
}
```

- ☐ A. Domain Controller
- ☐ B. Log collection server
- ☐ C. Database server
- ☒ D. Bastion host ✓

Explanation :

Answer – D



The bastion host needs a minimum configuration and a public IP address. The above CloudFormation template best fits this.

For more information on CloudFormation please visit the below link

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-what-is-concepts.html> (<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-what-is-concepts.html>)

Ask our Experts



QUESTION 74

UNATTEMPTED

DATA STORAGE

A recent increase in a number of users of an application hosted on an EC2 instance that you manage has caused the instance's OS to run out of CPU resources and crash. The crash caused several users' unsaved data to be lost and your supervisor wants to know how this problem can be avoided in the future. Which of the following would you not recommend?

Choose the correct answer from the below options:

- ☐ A. Redesign the application so that users' unsaved data is periodically written to disk.
- ☐ B. Take frequent snapshots of the EBS volume during business hours to ensure users' data is backed up. ✓
- ☐ C. Snapshot the EBS volume and re-deploy the application server as a larger instance type.
- ☐ D. Use autoscaling to deploy additional application server instances when load is high.

Explanation :

Answer – B



Option A is incorrect because this option would ensure that the user's unsaved data gets preserved just in case the instance crashes.

Option B is CORRECT because taking frequent snapshots of the EBS volume during business hours may cause data loss (losing the data that is not yet written to the volume that is being backed up via snapshot) . It is strongly recommended by AWS to either detach the volume or freeze all writes before taking the snapshot to prevent data loss. Hence, this option is certainly not recommended.

Option C is incorrect because using larger instance type can mitigate the problem of instance running out CPU.

Option D is incorrect because AutoScaling will ensure that that at least one (or minimum number of) instance(s) would be running to ensure that the application is always up and running.

For more information on EBS snapshots, please refer to the below URL:

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

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

<https://forums.aws.amazon.com/thread.jspa?threadID=92160>

(<https://forums.aws.amazon.com/thread.jspa?threadID=92160>)

Ask our Experts



QUESTION 75

UNATTEMPTED

DEPLOYMENT MANAGEMENT

Why will the following CloudFormation template fail to deploy a stack?

Choose the correct answer from the below options:

```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Parameters": {  
    "VPCId": {  
      "Type": "String",
```



```
"Description" : "Enter current VPC Id"

},

"SubnetId" : {

  "Type": "String",

  "Description" : "Enter a subnet Id"

}

},

"Outputs" : {

  "InstanceId" : {

    "Value" : { "Ref" : "MyInstance" },

    "Description" : "Instance Id"

  }

}

}
```

- ☐ A. CloudFormation templates do not use a "Parameters" section
- ☐ B. A "Conditions" section is mandatory but is not included
- ☒ C. A "Resources" section is mandatory but is not included ✓
- ☐ D. A template description is mandatory but is not included

Explanation :

Answer – C

Option C is CORRECT because, the Resources section is mandatory for the CloudFormation template to work; and it is missing in this template.

For more information on CloudFormation templates, please refer to the below URL:



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

Ask our Experts



QUESTION 76

UNATTEMPTED

HIGH AVAILABILITY AND BUSINESS CONTINUITY

You are maintaining an application that is spread across multiple web servers and has incoming traffic balanced by ELB. The application allows users to upload pictures. Currently, each web server stores the image and a background task synchronizes the data between servers. However, the synchronization task can no longer keep up with the number of images uploaded.

What change could you make so that all web servers have a place to store and read images at the same time?

Choose an answer from the below options:

- ☒ A. Store the images in Amazon S3. ✓
- ☐ B. Store the images on Amazon CloudFront.
- ☐ C. Store the images on Amazon EBS.
- ☐ D. Store the images on the ELB.

Explanation :

Answer – A

Option A is CORRECT because S3 provides a durable, secure, cost effective, and highly available storage service for the uploaded pictures.



Option B is incorrect because the application needs just a storage solution, not a global content distribution service. CloudFront is also costlier solution compared to S3.

Option C is incorrect because you cannot share EBS volumes among multiple EC2 instances.

Option D is incorrect because ELB cannot be used as a storage service.

For more information on AWS S3, please refer to the below URL:

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

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

Ask our Experts



QUESTION 77

UNATTEMPTED

DATA STORAGE

Which of the following is an example of a good Amazon DynamoDB hash key schema for provisioned throughput efficiency?

Choose an answer from the below options:

- ☐ A. Student ID where every student has a unique ID. ✓
- ☐ B. College ID where there are two colleges in the university.
- ☐ C. Class ID where every student is in one of the four classes.
- ☐ D. Tuition Plan where the vast majority of students are in state and the rest are out of state.

Explanation :

Answer – A

Option A is CORRECT because DynamoDB stores and retrieves each item based on the primary key (hash key) value which must be unique. Every student would surely have Student ID, hence, the data would be partitioned for each ID, which will make the data retrieval efficient.



Option B is incorrect because the data should spread evenly across all partitions for best throughput. With only two colleges, there would be only two partitions. This will not be as efficient as making Student ID the hash key.

Option C is incorrect because partitioning on Class ID will not be as efficient as doing so on the Student ID.

Option D is incorrect because there are only two possible options: in-state and out-of-state. This will not be as efficient as making Student ID the hash key.

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

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

Ask our Experts



QUESTION 78

UNATTEMPTED

SECURITY

Which of the below-mentioned ways can be used to provide additional layers of protection to all your EC2 resources?

Choose the correct answer from the below options:

- ☐ A. Add policies which have deny and/or allow permissions on tagged resources.
- ☐ B. Ensure that the proper tagging strategies have been implemented to identify all of your EC2 resources.
- ☐ C. Add an IP address condition to policies that specify that requests to EC2 instances should come from a specific IP address or CIDR block range.
- ☒ D. All actions listed here would provide additional layers of protection. ✓

Explanation :

Answer - D



Tagging allows you to understand which resources belong to test, development and production environment if done properly. 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.

If you have tagging, you can then also allow permissions based on the tags.

You can also use IP Address conditions in IAM policies for denying access to AWS resources.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": { "NotIpAddress": { "aws:SourceIp": [
      "192.0.2.0/24",
      "203.0.113.0/24"
    ] } }
  }
}
```

Options A, B, and C all provide additional layer of protection to the EC2 instances. Hence, D is the best answer.

For more information on tagging please see the below link:

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 79

UNATTEMPTED

SECURITY

Which of the following are correct statements with policy evaluation logic in AWS Identity and Access Management?

Choose 2 answers from the below options:



- ☐ A. An explicit deny does not override an explicit allow.
- ☐ B. By default, all request are allowed.
- ☐ C. An explicit allow overrides default deny. ✓
- ☐ D. An explicit allow overrides an explicit deny.
- ☐ E. By default, all requests are denied. ✓

Explanation :

Answer - C and E

Option A is incorrect because explicit deny always override an explicit allow.

Option B is incorrect because all requests are denied by default.

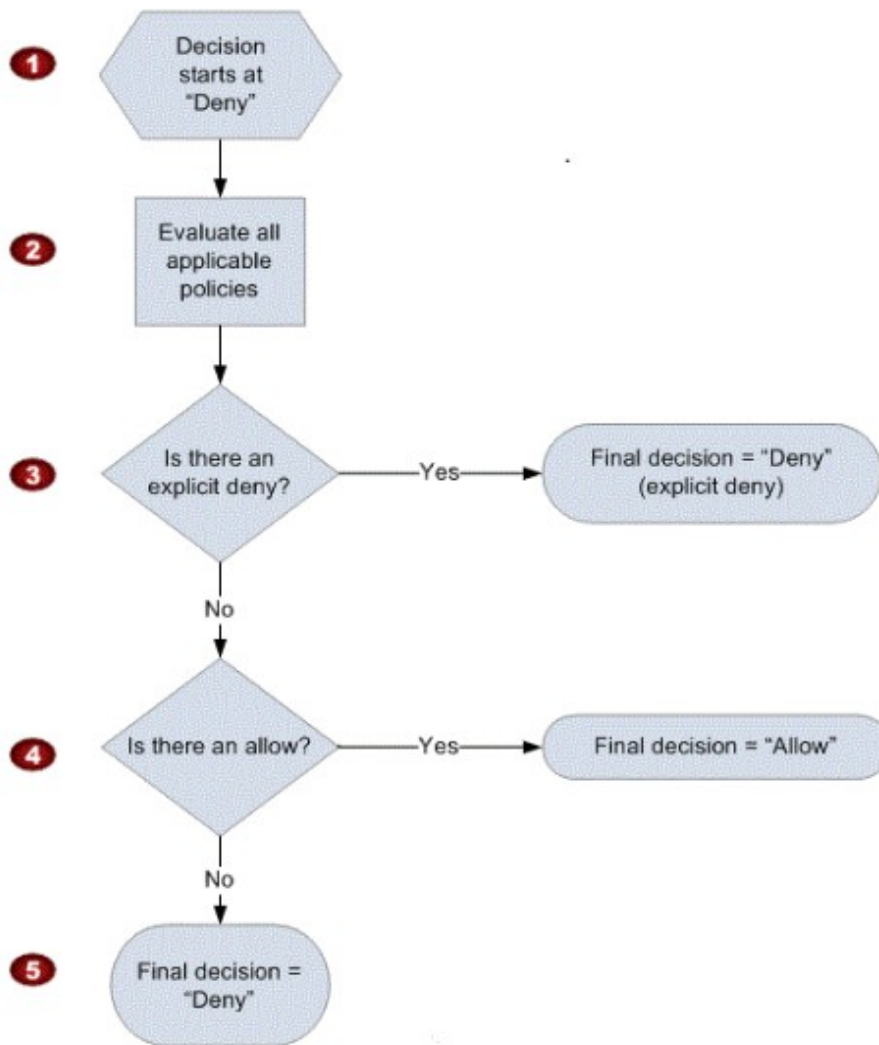
Option C is CORRECT because an explicit allow overrides the default deny.

Option D is incorrect because explicit deny cannot be overridden by an explicit allow.

Option E is CORRECT because all requests are denied by default.

The below diagram shows the evaluation logic of IAM policies. And as per the evaluation logic, it is clear that the above scenario leads to a default deny.





For more information on the IAM policy evaluation logic, please refer to the link http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html)

Ask our Experts



A company has developed a sensor intended to be placed inside of people's watches, monitoring the number of steps taken every day. There is an expectation of thousands of sensors reporting in every minute and hopes to scale to millions by the end of the year. A requirement for the project is it needs to be able to accept the data, run it through ETL to store in warehouse and archive it on Amazon Glacier, with room for a real-time dashboard for the sensor data to be added at a later date. What is the best method for architecting this application given the requirements?

Choose the correct answer from the below options:

- ☐ A. Write the sensor data to Amazon S3 with a lifecycle policy for Glacier, create an EMR cluster that uses the bucket data and runs it through ETL. It then outputs that data into Redshift data warehouse.
- ☐ B. Use Amazon Cognito to accept the data when the user pairs the sensor to the phone, and then have Cognito send the data to DynamoDB. Use Data Pipeline to create a job that takes the DynamoDB table and sends it to an EMR cluster for ETL, then outputs to Redshift and S3 while, using S3 lifecycle policies to archive on Glacier.
- ☐ C. Write the sensor data directly to a saleable DynamoDB; create a data pipeline that starts an EMR cluster using data from DynamoDB and sends the data to S3 and Redshift.
- ☐ D. Write the sensor data directly to Amazon Kinesis and output the data into Amazon S3 creating a lifecycle policy for Glacier archiving. Also, have a parallel processing application that runs the data through EMR and sends to a Redshift data warehouse. ✓

Explanation :

Answer – D

Option A is incorrect because S3 is not ideal for handling huge amount of real time requests.

Option B is incorrect because Amazon Cognito is not suitable for handling real time data.

Option C is incorrect because DynamoDB is not suitable for data ingestion and handling.



Option D is CORRECT because the requirement is real time data ingestion and analytics. The best option is to use Kinesis for storing the real time incoming data. The data can then be moved to S3 and then analyzed using EMR and Redshift. Data can then be moved to Glacier for archival.

More information about the use of Amazon Kinesis:

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

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

More information about the use of Amazon Cognito:

Amazon Cognito lets you easily add user sign-up and sign-in and manage permissions for your mobile and web apps. You can create your own user directory within Amazon Cognito, or you can authenticate users through social identity providers such as Facebook, Twitter, or Amazon; with SAML identity solutions; or by using your own identity system. In addition, Amazon Cognito enables you to save data locally on users' devices, allowing your applications to work even when the devices are offline. You can then synchronize data across users' devices so that their app experience remains consistent regardless of the device they use.

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csap-practice-tests/quiz/13607>)



Certification

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

Mobile App



Android Coming Soon



iOS Coming Soon

Company

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

Follow us



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



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



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



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

