Amazon

Exam Questions AWS-Solution-Architect-Associate

Amazon AWS Certified Solutions Architect - Associate

NEW QUESTION 1
In Amazon EC2 Container Service components, what is the name of a logical grouping of container instances on which you can place tasks?

A. A cluster
B. A container instance
C. A container
D. A task definition

Answer: A

Explanation:
Amazon ECS contains the following components:
A Cluster is a logical grouping of container instances that you can place tasks on.
A Container instance is an Amazon EC2 instance that is running the Amazon ECS agent and has been registered into a cluster.
A Task definition is a description of an application that contains one or more container definitions. A Scheduler is the method used for placing tasks on container instances.
A Service is an Amazon ECS service that allows you to run and maintain a specified number of instances of a task definition simultaneously.
A Task is an instantiation of a task definition that is running on a container instance. A Container is a Linux container that was created as part of a task.
Reference: http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

NEW QUESTION 2
In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately?

A. Because most reachability issues are resolved by automated processes in less than 20 minutes
B. Because all EC2 instances are unreachable for 20 minutes every day when AWS does routine maintenance
C. Because all EC2 instances are unreachable for 20 minutes when first launched
D. Because of all the reasons listed here

Answer: A

Explanation:
An EC2 instance must be unreachable for 20 minutes before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 minutes and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support.
Reference: https://aws.amazon.com/premiumsupport/faqs/

NEW QUESTION 3
One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?

A. Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locall
B. Gateway-stored enables you to configure youron-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.
C. Gateway-cached is free whilst gateway-stored is not.
D. Gateway-cached is up to 10 times faster than gateway-stored.
E. Gateway-stored lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locall
F. Gateway-cached enables you to configure youron-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

Answer: A

Explanation:
Volume gateways provide cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application sewers. The gateway supports the following volume configurations:
Gateway-cached volumes — You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data.
Gateway-stored volumes — If you need low-latency access to your entire data set, you can configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.
Reference: http://docs.aws.amazon.com/storagegateway/latest/userguide/volume-gateway.html

NEW QUESTION 4
A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

A. Always select the AZ while launching an instance
B. Always select the US-East-1-a zone for HA
C. Do not select the AZ; instead let AWS select the AZ
D. The user can never select the availability zone while launching an instance

Answer: C

Explanation:
When launching an instance with EC2, AWS recommends not to select the availability zone (AZ). AWS specifies that the default Availability Zone should be accepted. This is because it enables AWS to select the best Availability Zone based on the system health and available capacity. If the user launches additional instances, only then an Availability Zone should be specified. This is to specify the same or different AZ from the running instances.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

NEW QUESTION 5
After setting up a Virtual Private Cloud (VPC) network, a more experienced cloud engineer suggests that to achieve low network latency and high network throughput you should look into setting up a placement group. You know nothing about this, but begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group?

A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.
B. A placement group can span multiple Availability Zones.
C. You can't move an existing instance into a placement group.
D. A placement group can span peered VPCs

Answer: B

Explanation:
A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network. 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.
Placement groups have the following limitations:
The name you specify for a placement group a name must be unique within your AWS account. A placement group can't span multiple Availability Zones.
Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed. We recommend using the same instance type for all instances in a placement group.
You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group.
A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. For more information about VPC peering connections, see VPC Peering in the Amazon VPC User Guide.
You can't move an existing instance into a placement group. You can create an AM from your existing instance, and then launch a new instance from the AMI into a placement group.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

NEW QUESTION 6
You are migrating an internal sewer on your DC to an EC2 instance with EBS volume. Your server disk usage is around 500GB so you just copied all your data to a 2TB disk to be used with AWS Import/Export. Where will the data be imported once it arrives at Amazon?

A. to a 2TB EBS volume
B. to an S3 bucket with 2 objects of 1TB
C. to an 500GB EBS volume
D. to an S3 bucket as a 2TB snapshot

Answer: B

Explanation:
An import to Amazon EBS will have different results depending on whether the capacity of your storage device is less than or equal to 1 TB or greater than 1 TB. The maximum size of an Amazon EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on Amazon S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.
Reference: http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html

NEW QUESTION 7
An edge location refers to which Amazon Web Service?

A. An edge location is refered to the network configured within a Zone or Region
B. An edge location is an AWS Region
C. An edge location is the location of the data center used for Amazon CIoudFront.
D. An edge location is a Zone within an AWS Region

Answer: C

Explanation:
Amazon CIoudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of sewers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location.
Amazon CIoudFront can cache static content at each edge location. This means that your popular static content (e.g., your site’s logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CIoudFront also helps you offload requests for such files from your origin sever — CIoudFront serves the cached copy when available and only makes a request to your origin server if the edge location receMng the browser’s request does not have a copy of the file.
Reference: http://aws.amazon.com/c|oudfront/

NEW QUESTION 8
Your supervisor has asked you to build a simple file synchronization service for your department. He doesn't want to spend too much money and he wants to be notified of any changes to files by email. What do you think would be the best Amazon service to use for the email solution?

A. Amazon SES
B. Amazon CIoudSearch
C. Amazon SWF
D. Amazon AppStream

Answer: A

Explanation:

File change notifications can be sent via email to users following the resource with Amazon Simple Email Service (Amazon SES), an easy-to-use, cost-effective email solution.
Reference: http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_fIesync_08.pdf

NEW QUESTION 9
Your manager has just given you access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between the VPNs is secure. Which of the following services would be best for providing a low-cost hub-and-spoke model for primary or backup connectMty between these remote offices?

A. Amazon C|oudFront
B. AWS Direct Connect
C. AWS C|oudHSM
D. AWS VPN CIoudHub

Answer: D

Explanation:
If you have multiple VPN connections, you can provide secure communication between sites using the
AWS VPN CIoudHub. The VPN CIoudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectMty between these remote offices.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CIoudHub.htmI

NEW QUESTION 10
In Amazon AWS, which of the following statements is true of key pairs?

A. Key pairs are used only for Amazon SDKs.
B. Key pairs are used only for Amazon EC2 and Amazon CIoudFront.
C. Key pairs are used only for Elastic Load Balancing and AWS IAM.
D. Key pairs are used for all Amazon service

Answer: B

Explanation:
Key pairs consist of a public and private key, where you use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CIoudFront.
Reference: http://docs.aws.amazon.com/generaI/latest/gr/aws-sec-cred-types.html

NEW QUESTION 10
A user has created an EBS volume with 1000 IOPS. What is the average IOPS that the user will get for most of the year as per EC2 SLA if the instance is attached to the EBS optimized instance?

A. 950
B. 990
C. 1000
D. 900

Answer: D

Explanation:
As per AWS SLA if the instance is attached to an EBS-Optimized instance, then the Provisioned IOPS volumes are designed to deliver within 10% of the provisioned IOPS performance 99.9% of the time in a given year. Thus, if the user has created a volume of 1000 IOPS, the user will get a minimum 900 IOPS 99.9% time of the year.
Reference: http://aws.amazon.com/ec2/faqs/

NEW QUESTION 11
You are in the process of creating a Route 53 DNS failover to direct traffic to two EC2 zones. Obviously, if one fails, you would like Route 53 to direct traffic to the other region. Each region has an ELB with some instances being distributed. What is the best way for you to configure the Route 53 health check?

A. Route 53 doesn't support ELB with an internal health check.You need to create your own Route 53 health check of the ELB
B. Route 53 natively supports ELB with an internal health chec
C. Turn "Eva|uate target health" off and "Associate with Health Check" on and R53 will use the ELB's internal health check.
D. Route 53 doesn't support ELB with an internal health chec
E. You need to associate your resource record set for the ELB with your own health check
F. Route 53 natively supports ELB with an internal health chec
G. Turn "Eva|uate target health" on and "Associate with Health Check" off and R53 will use the ELB's internal health check.

Answer: D

Explanation:
With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your application is operating properly. When you enable this feature, Route 53 uses health checks-regularly making Internet requests to your application’s endpoints from multiple locations around the world-to determine whether each endpoint of your application is up or down.
To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route 53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB.
Reference:
http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb-integration-for-dns- fai|over/

NEW QUESTION 12
An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular EC2 instance, and it remains associated with your account until you choose to explicitly release it. By default how many EIPs is each AWS account limited to on a per region basis?

A. 1
B. 5
C. Unlimited
D. 10

Answer: B

Explanation:
By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames for all other inter-node communication.
If you feel your architecture warrants additional EIPs, you would need to complete the Amazon EC2 Elastic IP Address Request Form and give reasons as to your need for additional addresses. Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-ad dressing-limit

NEW QUESTION 13
While using the EC2 GET requests as URLs, the is the URL that serves as the entry point for the web service.

A. token
B. endpoint
C. action
D. None of these

Answer: B

Explanation:
The endpoint is the URL that serves as the entry point for the web service.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-query-api.html

NEW QUESTION 18
In DynamoDB, could you use IAM to grant access to Amazon DynamoDB resources and API actions?

A. In DynamoDB there is no need to grant access
B. Depended to the type of access
C. No
D. Yes

Answer: D

Explanation:
Amazon DynamoDB integrates with AWS Identity and Access Management (IAM). You can use AWS IAM to grant access to Amazon DynamoDB resources and API actions. To do this, you first write an AWS IAM policy, which is a document that explicitly lists the permissions you want to grant. You then attach that policy to an AWS IAM user or role.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/UsingIAMWithDDB.html

NEW QUESTION 22
is a fast, filexible, fully managed push messaging service.

A. Amazon SNS
B. Amazon SES
C. Amazon SQS
D. Amazon FPS

Answer: A

Explanation:
Amazon Simple Notification Service (Amazon SNS) is a fast, filexible, fully managed push messaging service. Amazon SNS makes it simple and cost-effective to push to mobile devices such as iPhone, iPad, Android, Kindle Fire, and internet connected smart devices, as well as pushing to other distributed services.
Reference: http://aws.amazon.com/sns/?nc1=h_I2_as

NEW QUESTION 26
In Amazon RDS, security groups are ideally used to:

A. Define maintenance period for database engines
B. Launch Amazon RDS instances in a subnet
C. Create, describe, modify, and delete DB instances
D. Control what IP addresses or EC2 instances can connect to your databases on a DB instance

Answer: D

Explanation:
In Amazon RDS, security groups are used to control what IP addresses or EC2 instances can connect to your databases on a DB instance.
When you first create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.

Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.html

NEW QUESTION 29
You have just been given a scope for a new client who has an enormous amount of data(petabytes) that he constantly needs analysed. Currently he is paying a huge amount of money for a data warehousing company to do this for him and is wondering if AWS can provide a cheaper solution. Do you think AWS has a solution for this?

A. Ye
B. Amazon SimpleDB
C. N
D. Not presently
E. Ye
F. Amazon Redshift
G. Ye
H. Your choice of relational AMIs on Amazon EC2 and EBS

Answer: C

Explanation:
Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. You can start small for just $0.25 per hour with no commitments or upfront costs and scale to a petabyte or more for $1,000 per terabyte per year, less than a tenth of most other data warehousing solutions. Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC drivers, allowing you to use a wide range of familiar SQL clients. Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host.
Reference: https://aws.amazon.com/running_databases/#redshift_anchor

NEW QUESTION 30
In an experiment, if the minimum size for an Auto Scaling group is 1 instance, which of the following statements holds true when you terminate the running instance?

A. Auto Scaling must launch a new instance to replace it.
B. Auto Scaling will raise an alarm and send a notification to the user for action.
C. Auto Scaling must configure the schedule actMty that terminates the instance after 5 days.
D. Auto Scaling will terminate the experimen

Answer: A

Explanation:
If the minimum size for an Auto Scaling group is 1 instance, when you terminate the running instance, Auto Scaling must launch a new instance to replace it.
Reference:http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

NEW QUESTION 33
A user has launched 10 EC2 instances inside a placement group. Which of the below mentioned statements is true with respect to the placement group?

A. All instances must be in the same AZ
B. All instances can be across multiple regions
C. The placement group cannot have more than 5 instances
D. All instances must be in the same region

Answer: A

Explanation:
A placement group is a logical grouping of EC2 instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network. Placement groups are recommended for applications that benefit from low network latency, high network throughput or both.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

NEW QUESTION 34
You log in to IAM on your AWS console and notice the following message. "Delete your root access keys." Why do you think IAM is requesting this?

A. Because the root access keys will expire as soon as you log out.
B. Because the root access keys expire after 1 week.
C. Because the root access keys are the same for all users.
D. Because they provide unrestricted access to your AWS resource

Answer: D

Explanation:
In AWS an access key is required in order to sign requests that you make using the command-line interface (CLI), using the AWS SDKs, or using direct API calls. Anyone who has the access key for your root account has unrestricted access to all the resources in your account, including billing information. One of the best ways to protect your account is to not have an access key for your root account. We recommend that unless you must have a root access key (this is very rare), that you do not generate one. Instead, AWS best practice is to create one or more AWS Identity and Access Management (IAM) users, give them the necessary permissions, and use IAM users for everyday interaction with AWS.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html#root-password

NEW QUESTION 38
Once again your customers are concerned about the security of their sensitive data and with their latest enquiry ask about what happens to old storage devices on

AWS. What would be the best answer to this QUESTION ?

A. AWS reformats the disks and uses them again.
B. AWS uses the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process.
C. AWS uses their own proprietary software to destroy data as part of the decommissioning process.
D. AWS uses a 3rd party security organization to destroy data as part of the decommissioning proces

Answer: B

Explanation:
When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized indMduals.
AWS uses the techniques detailed in DoD 5220.22-M ("Nationa| Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process.
All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance
with industry-standard practices.
Reference: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

NEW QUESTION 43
Your company has been storing a lot of data in Amazon Glacier and has asked for an inventory of what is in there exactly. So you have decided that you need to download a vault inventory. Which of the following statements is incorrect in relation to Vault Operations in Amazon Glacier?

A. You can use Amazon Simple Notification Service (Amazon SNS) notifications to notify you when the job completes.
B. A vault inventory refers to the list of archives in a vault.
C. You can use Amazon Simple Queue Service (Amazon SQS) notifications to notify you when the job completes.
D. Downloading a vault inventory is an asynchronous operatio

Answer: C

Explanation:
Amazon Glacier supports various vault operations.
A vault inventory refers to the list of archives in a vault. For each archive in the list, the inventory provides archive information such as archive ID, creation date, and size. Amazon Glacier updates the vault inventory approximately once a day, starting on the day the first archive is uploaded to the vault. A vault inventory must exist for you to be able to download it.
Downloading a vault inventory is an asynchronous operation. You must first initiate a job to download the inventory. After receMng the job request, Amazon Glacier prepares your inventory for download. After the job completes, you can download the inventory data.
Given the asynchronous nature of the job, you can use Amazon Simple Notification Service (Amazon SNS) notifications to notify you when the job completes. You can specify an Amazon SNS topic for each indMdual job request or configure your vault to send a notification when specific vault events occur. Amazon Glacier prepares an inventory for each vault periodically, every 24 hours. If there have been no archive additions or deletions to the vault since the last inventory, the inventory date is not updated. When you initiate a job for a vault inventory, Amazon Glacier returns the last inventory it generated, which is a point-in-time snapshot and not real-time data. You might not find it useful to retrieve vault inventory for each archive upload. However, suppose you maintain a database on the client-side associating metadata about the archives you upload to Amazon Glacier. Then, you might find the vault inventory useful to reconcile information in your database with the actual vault inventory.
Reference: http://docs.aws.amazon.com/amazongIacier/latest/dev/working-with-vaults.html

NEW QUESTION 45
AWS CIoudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CIoudFormation takes care of provisioning and configuring those resources for you. What formatting is required for this template?

A. JSON-formatted document
B. CSS-formatted document
C. XML-formatted document
D. HTML-formatted document

Answer: A

Explanation:
You can write an AWS CIoudFormation template (a JSON-formatted document) in a text editor or pick an existing template. The template describes the resources you want and their settings. For example,
suppose you want to create an Amazon EC2. Your template can declare an instance Amazon EC2 and describe its properties, as shown in the following example:
{
"AWSTemp|ateFormatVersion" : "2010-09-O9",
"Description" : "A simple Amazon EC2 instance", "Resources" : {
"MyEC2Instance" : {
"Type" : "AWS::EC2::Instance", "Properties" : {
"Image|d" : "ami-2f726546", "|nstanceType" : "t1.micro"
}
}
}
}
Reference:
http://docs.aws.amazon.com/AWSCIoudFormation/latest/UserGuide/cfn-whatis-howdoesitwork.html

NEW QUESTION 47
You decide that you need to create a number of Auto Scaling groups to try and save some money as you have noticed that at certain times most of your EC2 instances are not being used. By default, what is the maximum number of Auto Scaling groups that AWS will allow you to create?

A. 12

B. Unlimited
C. 20
D. 2

Answer: C

Explanation:
Auto Scaling is an AWS service that allows you to increase or decrease the number of EC2 instances within your application's architecture. With Auto Scaling, you create collections of EC2 instances, called Auto Scaling groups. You can create these groups from scratch, or from existing EC2 instances that are already in production.
Reference: http://docs.aws.amazon.com/general/latest/gr/aws_service_|imits.htm|#limits_autoscaling

NEW QUESTION 48
Which of the following is NOT a characteristic of Amazon Elastic Compute Cloud (Amazon EC2)?

A. It can be used to launch as many or as few virtual servers as you need.
B. It increases the need to forecast traffic by providing dynamic IP addresses for static cloud computing.
C. It eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
D. It offers scalable computing capacity in the Amazon Web Services (AWS) clou

Answer: B

Explanation:
Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you
to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

NEW QUESTION 51
You are setting up your first Amazon Virtual Private Cloud (Amazon VPC) so you decide to use the VPC wizard in the AWS console to help make it easier for you. Which of the following statements is correct regarding instances that you launch into a default subnet via the VPC wizard?

A. Instances that you launch into a default subnet receive a public IP address and 10 private IP addresses.
B. Instances that you launch into a default subnet receive both a public IP address and a private IP address.
C. Instances that you launch into a default subnet don't receive any ip addresses and you need to define them manually.
D. Instances that you launch into a default subnet receive a public IP address and 5 private IP addresse

Answer: B

Explanation:
Instances that you launch into a default subnet receive both a public IP address and a private IP address. Instances in a default subnet also receive both public and private DNS hostnames. Instances that you launch into a nondefault subnet in a default VPC don't receive a public IP address or a DNS hostname. You can change your subnet's default public IP addressing behavior.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/default-vpc.html

NEW QUESTION 52
Amazon S3 allows you to set per-file permissions to grant read and/or write access. However you have decided that you want an entire bucket with 100 files already in it to be accessible to the public. You don't want to go through 100 files indMdually and set permissions. What would be the best way to do this?

A. Move the bucket to a new region
B. Add a bucket policy to the bucket.
C. Move the files to a new bucket.
D. Use Amazon EBS instead of S3

Answer: B

Explanation:
Amazon S3 supports several mechanisms that give you filexibility to control who can access your data as well as how, when, and where they can access it. Amazon S3 provides four different access control mechanisms: AWS Identity and Access Management (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication. IAM enables organizations to create and manage multiple users under a single AWS account. With IAM policies, you can grant IAM users fine-grained control to your Amazon S3 bucket or objects. You can use ACLs to selectively add (grant) certain permissions on indMdual objects. Amazon S3 bucket policies can be used to add or deny permissions across some or all of the objects within a single bucket.
With Query string authentication, you have the ability to share Amazon S3 objects through URLs that are
valid for a specified period of time.
Reference: http://aws.amazon.com/s3/detai|s/#security

NEW QUESTION 53
Which of the following statements is true of creating a launch configuration using an EC2 instance?

A. The launch configuration can be created only using the Query APIs.
B. Auto Scaling automatically creates a launch configuration directly from an EC2 instance.
C. A user should manually create a launch configuration before creating an Auto Scaling group.
D. The launch configuration should be created manually from the AWS CL

Answer: B

Explanation:

You can create an Auto Scaling group directly from an EC2 instance. When you use this feature, Auto Scaling automatically creates a launch configuration for you as well.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveIoperGuide/create-Ic-with-instancelD.htmI

NEW QUESTION 55
You have been using T2 instances as your CPU requirements have not been that intensive. However you now start to think about larger instance types and start looking at M and IV|3 instances. You are a little confused as to the differences between them as they both seem to have the same ratio of CPU and memory. Which statement below is incorrect as to why you would use one over the other?

A. M3 instances are less expensive than M1 instances.
B. IV|3 instances are configured with more swap memory than M instances.
C. IV|3 instances provide better, more consistent performance that M instances for most use-cases.
D. M3 instances also offer SSD-based instance storage that delivers higher I/O performanc

Answer: B

Explanation:
Amazon EC2 allows you to set up and configure everything about your instances from your operating system up to your applications. An Amazon Nlachine Image (AMI) is simply a packaged-up environment that includes all the necessary bits to set up and boot your instance.
M1 and M3 Standard instances have the same ratio of CPU and memory, some reasons below as to why you would use one over the other.
IV|3 instances provide better, more consistent performance that M instances for most use-cases. M3 instances also offer SSD-based instance storage that delivers higher I/O performance.
M3 instances are also less expensive than M1 instances. Due to these reasons, we recommend M3 for applications that require general purpose instances with a balance of compute, memory, and network resources.
However, if you need more disk storage than what is provided in M3 instances, you may still find M1 instances useful for running your applications.
Reference: https://aws.amazon.com/ec2/faqs/

NEW QUESTION 59
You have set up an Elastic Load Balancer (ELB) with the usual default settings, which route each request independently to the application instance with the smallest load. However, someone has asked you to bind a user's session to a specific application instance so as to ensure that all requests coming from the user during the session will be sent to the same application instance. AWS has a feature to do this. What is it called?

A. Connection draining
B. Proxy protocol
C. Tagging
D. Sticky session

Answer: D

Explanation:
An Elastic Load BaIancer(ELB) by default, routes each request independently to the application instance
with the smallest load. However, you can use the sticky session feature (also known as session affinity), which enables the load balancer to bind a user's session to a specific application instance. This ensures that all requests coming from the user during the session will be sent to the same application instance. The key to managing the sticky session is determining how long your load balancer should consistently route the user's request to the same application instance. If your application has its own session cookie, then you can set Elastic Load Balancing to create the session cookie to follow the duration specified by the application's session cookie. If your application does not have its own session cookie, then you can set Elastic Load Balancing to create a session cookie by specifying your own stickiness duration. You can associate stickiness duration for only HTTP/HTTPS load balancer listeners.
An application instance must always receive and send two cookies: A cookie that defines the stickiness duration and a special Elastic Load Balancing cookie named AWSELB, that has the mapping to the application instance.
Reference: http://docs.aws.amazon.com/E|asticLoadBaIancing/latest/DeveIoperGuide/TerminoIogyandKeyConcepts. htmI#session-stickiness

NEW QUESTION 61
A user wants to achieve High Availability with PostgreSQL DB. Which of the below mentioned functionalities helps achieve HA?

A. Mu|ti AZ
B. Read Replica
C. Multi region
D. PostgreSQL does not support HA

Answer: A

Explanation:
The Multi AZ feature allows the user to achieve High Availability. For Multi AZ, Amazon RDS automatically provisions and maintains a synchronous "standby" replica in a different Availability Zone. Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

NEW QUESTION 63
You are building a system to distribute confidential documents to employees. Using CIoudFront, what method could be used to serve content that is stored in S3, but not publically accessible from S3 directly?

A. Add the CIoudFront account security group "amazon-cf/amazon-cf-sg" to the appropriate S3 bucket policy.
B. Create a S3 bucket policy that lists the C|oudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).
C. Create an Identity and Access Management (IAM) User for CIoudFront and grant access to the objects in your S3 bucket to that IAM User.
D. Create an Origin Access Identity (OAI) for CIoudFront and grant access to the objects in your S3 bucket to that OAI.

Answer: D

Explanation:
You restrict access to Amazon S3 content by creating an origin access identity, which is a special CIoudFront user. You change Amazon S3 permissions to give

the origin access identity permission to access your objects, and to remove permissions from everyone else. When your users access your Amazon S3 objects using CIoudFront URLs, the CIoudFront origin access identity gets the objects on your users' behalf. If your users try to access objects using Amazon S3 URLs, they're denied access. The origin access identity has permission to access objects in your Amazon S3 bucket, but users don't. Reference: http://docs.aws.amazon.com/AmazonCIoudFront/latest/Deve|operGuide/private-content-restricting-acces s-to-s3.html

NEW QUESTION 67
A user has attached 1 EBS volume to a VPC instance. The user wants to achieve the best fault tolerance of data possible. Which of the below mentioned options can help achieve fault tolerance?

A. Attach one more volume with RAID 1 configuration.
B. Attach one more volume with RAID 0 configuration.
C. Connect multiple volumes and stripe them with RAID 6 configuration.
D. Use the EBS volume as a root devic

Answer: A

Explanation:
The user can join multiple provisioned IOPS volumes together in a RAID 1 configuration to achieve better fault tolerance. RAID 1 does not provide a write performance improvement; it requires more bandwidth than non-RAID configurations since the data is written simultaneously to multiple volumes. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

NEW QUESTION 68
A user is aware that a huge download is occurring on his instance. He has already set the Auto Scaling policy to increase the instance count when the network I/O increases beyond a certain limit. How can the user ensure that this temporary event does not result in scaling?

A. The network I/O are not affected during data download
B. The policy cannot be set on the network I/O
C. There is no way the user can stop scaling as it is already configured
D. Suspend scaling

Answer: D

Explanation:
The user may want to stop the automated scaling processes on the Auto Scaling groups either to perform manual operations or during emergency situations. To perform this, the user can suspend one or more scaling processes at any time. Once it is completed, the user can resume all the suspended processes. Reference:http://docs.aws.amazon.com/AutoScaIing/latest/Deve|operGuide/AS_Concepts.htmI

NEW QUESTION 73
An accountant asks you to design a small VPC network for him and, due to the nature of his business, just needs something where the workload on the network will be low, and dynamic data will be accessed infrequently. Being an accountant, low cost is also a major factor. Which EBS volume type would best suit his requirements?

A. Magnetic
B. Any, as they all perform the same and cost the same.
C. General Purpose (SSD)
D. Magnetic or Provisioned IOPS (SSD)

Answer: A

Explanation:
You can choose between three EBS volume types to best meet the needs of their workloads: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic. General Purpose (SSD) is the new, SSD-backed, general purpose EBS volume type that we recommend as the default choice for customers. General Purpose (SSD) volumes are suitable for a broad range of workloads, including small to medium sized databases, development and test environments, and boot volumes. Provisioned IOPS (SSD) volumes offer storage with consistent and low-latency performance, and are designed for I/O intensive applications such as large relational or NoSQL databases. Magnetic volumes provide the lowest cost per gigabyte of all EBS volume types. Magnetic volumes are ideal for workloads where data is accessed infrequently, and applications where the lowest storage cost is important.
Reference: https://aws.amazon.com/ec2/faqs/

NEW QUESTION 76
A user is planning to launch a scalable web application. Which of the below mentioned options will not affect the latency of the application?

A. Region.
B. Provisioned IOPS.
C. Availability Zone.
D. Instance siz

Answer: C

Explanation:
In AWS, the instance size decides the I/O characteristics. The provisioned IOPS ensures higher throughput, and lower latency. The region does affect the latency; latency will always be less when the instance is near to the end user. Within a region the user uses any AZ and this does not affect the latency. The AZ is mainly for fault toleration or HA.
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

NEW QUESTION 79
Do you need to shutdown your EC2 instance when you create a snapshot of EBS volumes that serve as root devices?

A. No, you only need to shutdown an instance before deleting it.

B. Yes
C. No, the snapshot would turn off your instance automatically.
D. No

Answer: B

Explanation:
Yes, to create a snapshot for Amazon EBS volumes that serve as root devices, you should stop the instance before taking the snapshot.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

NEW QUESTION 81
A user is running a batch process which runs for 1 hour every day. Which of the below mentioned options is the right instance type and costing model in this case if the user performs the same task for the whole year?

A. EBS backed instance with on-demand instance pricing.
B. EBS backed instance with heavy utilized reserved instance pricing.
C. EBS backed instance with low utilized reserved instance pricing.
D. Instance store backed instance with spot instance pricin

Answer: A

Explanation:
For Amazon Web Services, the reserved instance helps the user save money if the user is going to run the same instance for a longer period. Generally if the user uses the instances around 30-40% annually it is recommended to use RI. Here as the instance runs only for 1 hour daily it is not recommended to have RI as it will be costlier. The user should use on-demand with EBS in this case.
Reference: http://aws.amazon.com/ec2/purchasing-options/reserved-instances/

NEW QUESTION 82
Which IAM role do you use to grant AWS Lambda permission to access a DynamoDB Stream?

A. Dynamic role
B. Invocation role
C. Execution role
D. Event Source role

Answer: C

Explanation:
You grant AWS Lambda permission to access a DynamoDB Stream using an IAM role known as the "execution ro|e".
Reference: http://docs.aws.amazon.com/|ambda/latest/dg/intro-permission-model.htm|

NEW QUESTION 83
A scope has been handed to you to set up a super fast gaming server and you decide that you will use Amazon DynamoDB as your database. For efficient access to data in a table, Amazon DynamoDB creates and maintains indexes for the primary key attributes. A secondary index is a data structure that contains a subset of attributes from a table, along with an alternate key to support Query operations. How many types of secondary indexes does DynamoDB support?

A. 2
B. 16
C. 4
D. As many as you nee

Answer: A

Explanation:
DynamoDB supports two types of secondary indexes:
Local secondary index — an index that has the same hash key as the table, but a different range key. A local secondary index is "local" in the sense that every partition of a local secondary index is scoped to a table partition that has the same hash key.
Global secondary index — an index with a hash and range key that can be different from those on the table. A global secondary index is considered "global" because queries on the index can span all of the data in a table, across all partitions.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html

NEW QUESTION 86
Select the correct statement: Within Amazon EC2, when using Linux instances, the device name
/dev/sda1 is .

A. reserved for EBS volumes
B. recommended for EBS volumes
C. recommended for instance store volumes
D. reserved for the root device

Answer: D

Explanation:
Within Amazon EC2, when using a Linux instance, the device name /dev/sda1 is reserved for the root device.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/device_naming.htmI

NEW QUESTION 88

A user has set up the CIoudWatch alarm on the CPU utilization metric at 50%, with a time interval of 5 minutes and 10 periods to monitor. What will be the state of the alarm at the end of 90 minutes, if the CPU utilization is constant at 80%?

A. ALERT
B. ALARM
C. OK
D. INSUFFICIENT_DATA

Answer: B

Explanation:
In this case the alarm watches a metric every 5 minutes for 10 intervals. Thus, it needs at least 50 minutes to come to the "OK" state.
Till then it will be in the |NSUFFUCIENT_DATA state.
Since 90 minutes have passed and CPU utilization is at 80% constant, the state of alarm will be "ALARNI". Reference:
http://docs.aws.amazon.com/AmazonCIoudWatch/latest/DeveloperGuide/AlarmThatSendsEmaiI.html

NEW QUESTION 90
A user is planning to make a mobile game which can be played online or offline and will be hosted on EC2.
The user wants to ensure that if someone breaks the highest score or they achieve some milestone they can inform all their colleagues through email. Which of the below mentioned AWS services helps achieve this goal?

A. AWS Simple Workflow Service.
B. AWS Simple Email Service.
C. Amazon Cognito
D. AWS Simple Queue Servic

Answer: B

Explanation:
Amazon Simple Email Service (Amazon SES) is a highly scalable and cost-effective email-sending service for businesses and developers. It integrates with other AWS services, making it easy to send emails from applications that are hosted on AWS.
Reference: http://aws.amazon.com/ses/faqs/

NEW QUESTION 93
You have multiple VPN connections and want to provide secure communication between sites using the AWS VPN CIoudHub. Which statement is the most accurate in describing what you must do to set this up correctly?

A. Create a virtual private gateway with multiple customer gateways, each with unique Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs)
B. Create a virtual private gateway with multiple customer gateways, each with a unique set of keys
C. Create a virtual public gateway with multiple customer gateways, each with a unique Private subnet
D. Create a virtual private gateway with multiple customer gateways, each with unique subnet id

Answer: A

Explanation:
If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CIoudHub. The VPN CIoudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectMty between these remote offices.
To use the AWS VPN CIoudHub, you must create a virtual private gateway with multiple customer
gateways, each with unique Border Gateway Protocol (BGP) Autonomous System Numbers (ASNs). Customer gateways advertise the appropriate routes (BGP prefixes) over their VPN connections. These routing advertisements are received and re-advertised to each BGP peer, enabling each site to send data to and receive data from the other sites. The routes for each spoke must have unique ASNs and the sites must not have overlapping IP ranges. Each site can also send and receive data from the VPC as if they were using a standard VPN connection.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CIoudHub.html

NEW QUESTION 98
While creating an Amazon RDS DB, your first task is to set up a DB that controls which IP address or EC2 instance can access your DB Instance.

A. security token pool
B. security token
C. security pool
D. security group

Answer: D

Explanation:
While creating an Amazon RDS DB, your first task is to set up a DB Security Group that controls what IP addresses or EC2 instances have access to your DB Instance.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithSecurityGroups.html

NEW QUESTION 99
Which one of the below is not an AWS Storage Service?

A. Amazon S3
B. Amazon Glacier
C. Amazon CIoudFront
D. Amazon EBS

Answer: C

Explanation:
AWS Storage Services are: Amazon S3
Amazon Glacier Amazon EBS
AWS Storage Gateway
Reference: https://console.aws.amazon.com/console

NEW QUESTION 103
A user has deployed an application on his private cloud. The user is using his own monitoring tool. He wants to configure it so that whenever there is an error, the monitoring tool will notify him via SMS. Which of the below mentioned AWS services will help in this scenario?

A. AWS SES
B. AWS SNS
C. None because the user infrastructure is in the private cloud.
D. AWS SMS

Answer: B

Explanation:
Amazon Simple Notification Service (Amazon SNS) is a fast, filexible, and fully managed push messaging service. Amazon SNS can be used to make push notifications to mobile devices. Amazon SNS can
deliver notifications by SMS text message or email to the Amazon Simple Queue Service (SQS) queues or to any HTTP endpoint. In this case user can use the SNS apis to send SMS.
Reference: http://aws.amazon.com/sns/

NEW QUESTION 108
Regarding Amazon Route 53, if your application is running on Amazon EC2 instances in two or more Amazon EC2 regions and if you have more than one Amazon EC2 instance in one or more regions, you can use to route traffic to the correct region and then use to route traffic to instances
within the region, based on probabilities that you specify.

A. weighted-based routing; alias resource record sets
B. latency-based routing; weighted resource record sets
C. weighted-based routing; weighted resource record sets
D. latency-based routing; alias resource record sets

Answer: B

Explanation:
Regarding Amazon Route 53, if your application is running on Amazon EC2 instances in two or more Amazon EC2 regions, and if you have more than one Amazon EC2 instance in one or more regions, you can use latency-based routing to route traffic to the correct region and then use weighted resource record sets to route traffic to instances within the region based on weights that you specify.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Tutorials.html

NEW QUESTION 111
You have a lot of data stored in the AWS Storage Gateway and your manager has come to you asking about how the billing is calculated, specifically the Virtual Tape Shelf usage. What would be a correct response to this?

A. You are billed for the virtual tape data you store in Amazon Glacier and are billed for the size of the virtual tape.
B. You are billed for the virtual tape data you store in Amazon Glacier and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
C. You are billed for the virtual tape data you store in Amazon S3 and billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
D. You are billed for the virtual tape data you store in Amazon S3 and are billed for the size of the virtual tape.

Answer: B

Explanation:
The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization’s on-premises IT environment and AWS’s storage infrastructure.
AWS Storage Gateway billing is as follows. Volume storage usage (per GB per month):
You are billed for the Cached volume data you store in Amazon S3. You are only billed for volume capacity you use, not for the size of the volume you create.
Snapshot Storage usage (per GB per month): You are billed for the snapshots your gateway stores in Amazon S3. These snapshots are stored and billed as Amazon EBS snapshots. Snapshots are incremental backups, reducing your storage charges. When taking a new snapshot, only the data that has changed since your last snapshot is stored.
Virtual Tape Library usage (per GB per month):
You are billed for the virtual tape data you store in Amazon S3. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
Virtual Tape Shelf usage (per GB per month):
You are billed for the virtual tape data you store in Amazon Glacier. You are only billed for the portion of virtual tape capacity that you use, not for the size of the virtual tape.
Reference: https://aws.amazon.com/storagegateway/faqs/

NEW QUESTION 113
You are configuring a new VPC for one of your clients for a cloud migration project, and only a public VPN will be in place. After you created your VPC, you created a new subnet, a new internet gateway, and attached your internet gateway to your VPC. When you launched your first instance into your VPC, you realized that you aren't able to connect to the instance, even if it is configured with an elastic IP. What should be done to access the instance?

A. A route should be created as 0.0.0.0/0 and your internet gateway as target.
B. Attach another ENI to the instance and connect via new ENI.
C. A NAT instance should be created and all traffic should be forwarded to NAT instance.
D. A NACL should be created that allows all outbound traffi

Answer: A

Explanation:
All traffic should be routed via Internet Gateway. So, a route should be created with 0.0.0.0/0 as a source, and your Internet Gateway as your target.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html

NEW QUESTION 118
You are setting up some EBS volumes for a customer who has requested a setup which includes a RAID (redundant array of inexpensive disks). AWS has some recommendations for RAID setups. Which RAID setup is not recommended for Amazon EBS?

A. RAID 5 only
B. RAID 5 and RAID 6
C. RAID 1 only
D. RAID 1 and RAID 6

Answer: B

Explanation:
With Amazon EBS, you can use any of the standard RAID configurations that you can use with a traditional bare metal server, as long as that particular RAID configuration is supported by the operating system for your instance. This is because all RAID is accomplished at the software level. For greater I/O performance than you can achieve with a single volume, RAID 0 can stripe multiple volumes together; for on-instance redundancy, RAID 1 can mirror two volumes together. RAID 5 and RAID 6 are not recommended for Amazon EBS because the parity write operations of these RAID modes consume some of the IOPS available to your volumes.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

NEW QUESTION 120
Doug has created a VPC with CIDR 10.201.0.0/16 in his AWS account. In this VPC he has created a public subnet with CIDR block 10.201.31.0/24. While launching a new EC2 from the console, he is not able to assign the private IP address 10.201.31.6 to this instance. Which is the most likely reason for this issue?

A. Private IP address 10.201.31.6 is blocked via ACLs in Amazon infrastructure as a part of platform security.
B. Private address IP 10.201.31.6 is currently assigned to another interface.
C. Private IP address 10.201.31.6 is not part of the associated subnet's IP address range.
D. Private IP address 10.201.31.6 is reserved by Amazon for IP networking purpose

Answer: B

Explanation:
In Amazon VPC, you can assign any Private IP address to your instance as long as it is: Part of the associated subnet's IP address range
Not reserved by Amazon for IP networking purposes Not currently assigned to another interface Reference: http://aws.amazon.com/vpc/faqs/

NEW QUESTION 125
You have been setting up an Amazon Virtual Private Cloud (Amazon VPC) for your company, including setting up subnets. Security is a concern, and you are not sure which is the best security practice for securing subnets in your VPC. Which statement below is correct in describing the protection of AWS resources in each subnet?

A. You can use multiple layers of security, including security groups and network access control lists (ACL).
B. You can only use access control lists (ACL).
C. You don't need any security in subnets.
D. You can use multiple layers of security, including security groups, network access control lists (ACL) and CIoudHSM.

Answer: A

Explanation:
A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.
To protect the AWS resources in each subnet, you can use multiple layers of security, including security groups and network access control lists (ACL).
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_|ntroduction.html

NEW QUESTION 126
A user has created a CIoudFormation stack. The stack creates AWS services, such as EC2 instances, ELB, AutoScaling, and RDS. While creating the stack it created EC2, ELB and AutoScaling but failed to create RDS. What will C|oudFormation do in this scenario?

A. Rollback all the changes and terminate all the created services
B. It will wait for the user's input about the error and correct the mistake after the input
C. CIoudFormation can never throw an error after launching a few services since it verifies all the steps before launching
D. It will warn the user about the error and ask the user to manually create RDS

Answer: A

Explanation:
AWS CIoudFormation is an application management tool which provides application modeling, deployment, configuration, management and related actMties. The AWS CIoudFormation stack is a collection of AWS resources which are created and managed as a single unit when AWS CIoudFormation instantiates a template. If any of the services fails to launch, C|oudFormation will rollback all the changes and terminate or delete all the created services.
Reference: http://aws.amazon.com/c|oudformation/faqs/

NEW QUESTION 128
You have just finshed setting up an advertisement server in which one of the obvious choices for a service was Amazon Elastic Map Reduce(EMR) and are now

troubleshooting some weird cluster states that you are seeing. Which of the below is not an Amazon EMR cluster state?

A. STARTING
B. STOPPED
C. RUNNING
D. WAITING

Answer: B

Explanation:
Amazon Elastic Map Reduce (EMR) is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data.
Amazon EMR historically referred to an Amazon EMR cluster (and all processing steps assigned to it) as a "c|uster". Every cluster has a unique identifier that starts with "j-".
The different cluster states of an Amazon EMR cluster are listed below. STARTING — The cluster provisions, starts, and configures EC2 instances.
BOOTSTRAPPING — Bootstrap actions are being executed on the cluster. RUNNING — A step for the cluster is currently being run.
WAITING — The cluster is currently active, but has no steps to run. TERMINATING - The cluster is in the process of shutting down. TERMINATED - The cluster was shut down without error. TERMINATED_W|TH_ERRORS - The cluster was shut down with errors.
Reference: https://aws.amazon.com/elasticmapreduce/faqs/

NEW QUESTION 129
Is it possible to get a history of all EC2 API calls made on your account for security analysis and operational troubleshooting purposes?

A. Yes, by default, the history of your API calls is logged.
B. Yes, you should turn on the CloudTrail in the AWS console.
C. No, you can only get a history of VPC API calls.
D. No, you cannot store history of EC2 API calls on Amazon.

Answer: B

Explanation:
To get a history of all EC2 API calls (including VPC and EBS) made on your account, you simply turn on C|oudTrai| in the AWS Management Console.
Reference: https://aws.amazon.com/ec2/faqs/

NEW QUESTION 133
You have just set up yourfirst Elastic Load Balancer (ELB) but it does not seem to be configured properly. You discover that before you start using ELB, you have to configure the listeners for your load balancer. Which protocols does ELB use to support the load balancing of applications?

A. HTTP and HTTPS
B. HTTP, HTTPS , TCP, SSL and SSH
C. HTTP, HTTPS , TCP, and SSL
D. HTTP, HTTPS , TCP, SSL and SFTP

Answer: C

Explanation:
Before you start using Elastic Load BaIancing(ELB), you have to configure the listeners for your load balancer. A listener is a process that listens for connection requests. It is configured with a protocol and a port number for front-end (client to load balancer) and back-end (load balancer to back-end instance) connections.
Elastic Load Balancing supports the load balancing of applications using HTTP, HTTPS (secure HTTP), TCP, and SSL (secure TCP) protocols. The HTTPS uses the SSL protocol to establish secure connections over the HTTP layer. You can also use SSL protocol to establish secure connections over the TCP layer.
The acceptable ports for both HTTPS/SSL and HTTP/TCP connections are 25, 80, 443, 465, 587, and
1024-65535.
Reference:
http://docs.aws.amazon.com/E|asticLoadBaIancing/latest/DeveIoperGuide/elb-listener-config.htmI

NEW QUESTION 137
After moving an E-Commerce website for a client from a dedicated server to AWS you have also set up auto scaling to perform health checks on the instances in your group and replace instances that fail these checks. Your client has come to you with his own health check system that he wants you to use as it has proved to be very useful prior to his site running on AWS. What do you think would be an appropriate response to this given all that you know about auto scaling?

A. It is not possible to implement your own health check syste
B. You need to use AWSs health check system.
C. It is not possible to implement your own health check system due to compatibility issues.
D. It is possible to implement your own health check system and then send the instance's health information directly from your system to Cloud Watch.
E. It is possible to implement your own health check system and then send the instance's health information directly from your system to Cloud Watch but only in the US East (
F. Virginia) region.

Answer: C

Explanation:
Auto Scaling periodically performs health checks on the instances in your group and replaces instances that fail these checks. By default, these health checks use the results of EC2 instance status checks to determine the health of an instance. If you use a load balancer with your Auto Scaling group, you can optionally choose to include the results of Elastic Load Balancing health checks.
Auto Scaling marks an instance unhealthy if the calls to the Amazon EC2 action DescribeInstanceStatus returns any other state other than running, the system status shows impaired, or the calls to Elastic Load Balancing action DescribeInstanceHealth returns OutOfService in the instance state field.
After an instance is marked unhealthy because of an Amazon EC2 or Elastic Load Balancing health check, it is scheduled for replacement.
You can customize the health check conducted by your Auto Scaling group by specifying additional checks or by having your own health check system and then sending the instance's health information directly from your system to Auto Scaling.
Reference: http://docs.aws.amazon.com/AutoScaling/latest/Deve|operGuide/healthcheck.html

NEW QUESTION 141
You havejust discovered that you can upload your objects to Amazon S3 using Multipart Upload API. You start to test it out but are unsure of the benefits that it would provide. Which of the following is not a benefit of using multipart uploads?

A. You can begin an upload before you know the final object size.
B. Quick recovery from any network issues.
C. Pause and resume object uploads.
D. It's more secure than normal uploa

Answer: D

Explanation:
Multipart upload in Amazon S3 allows you to upload a single object as a set of parts. Each part is a contiguous portion ofthe object's data. You can upload these object parts independently and in any order.
If transmission of any part fails, you can re-transmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when
your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.
Using multipart upload provides the following advantages:
Improved throughput—You can upload parts in parallel to improve throughput.
Quick recovery from any network issues—Smaller part size minimizes the impact of restarting a failed upload due to a network error.
Pause and resume object uploads—You can upload object parts over time. Once you initiate a multipart upload there is no expiry; you must explicitly complete or abort the multipart upload.
Begin an upload before you know the final object size—You can upload an object as you are creating it. Reference:
http://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

NEW QUESTION 143
What happens to Amazon EBS root device volumes, by default, when an instance terminates?

A. Amazon EBS root device volumes are moved to IAM.
B. Amazon EBS root device volumes are copied into Amazon RDS.
C. Amazon EBS root device volumes are automatically deleted.
D. Amazon EBS root device volumes remain in the database until you delete the

Answer: C

Explanation:
By default, Amazon EBS root device volumes are automatically deleted when the instance terminates. Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html

NEW QUESTION 144
A favored client needs you to quickly deploy a database that is a relational database service with minimal administration as he wants to spend the least amount of time administering it. Which database would be the best option?

A. Amazon Simp|eDB
B. Your choice of relational AMs on Amazon EC2 and EBS.
C. Amazon RDS
D. Amazon Redshift

Answer: C

Explanation:
Amazon Relational Database Service (Amazon RDS) is a web service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks, freeing you up to focus on your applications and business.
Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user-defined retention period and enabling point-in-time recovery.
Reference: https://aws.amazon.com/running_databases/#rds_anchor

NEW QUESTION 149
You are setting up some IAM user policies and have also become aware that some services support resource-based permissions, which let you attach policies to the service's resources instead of to IAM users or groups. Which of the below statements is true in regards to resource-level permissions?

A. All services support resource-level permissions for all actions.
B. Resource-level permissions are supported by Amazon CIoudFront
C. All services support resource-level permissions only for some actions.
D. Some services support resource-level permissions only for some action

Answer: D

Explanation:
AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
In addition to supporting IAM user policies, some services support resource-based permissions, which let you attach policies to the service's resources instead of to IAM users or groups. Resource-based permissions are supported by Amazon S3, Amazon SNS, and Amazon SQS.
The resource-level permissions service supports IAM policies in which you can specify indMdual resources using Amazon Resource Names (ARNs) in the poIicy's Resource element.

Some services support resource-level permissions only for some actions.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SpecificProducts.html

NEW QUESTION 152
In relation to AWS CloudHSM, High-availability (HA) recovery is hands-off resumption by failed HA group members.
Prior to the introduction of this function, the HA feature provided redundancy and performance, but required that a failed/lost group member be reinstated.

A. automatically
B. periodically
C. manually
D. continuosly

Answer: C

Explanation:
In relation to AWS CloudHS|VI, High-availability (HA) recovery is hands-off resumption by failed HA group members.
Prior to the introduction of this function, the HA feature provided redundancy and performance, but required that a failed/lost group member be manually reinstated.
Reference: http://docs.aws.amazon.com/cloudhsm/latest/userguide/ha-best-practices.html

NEW QUESTION 157
You are using Amazon SES as an email solution but are unsure of what its limitations are. Which statement below is correct in regards to that?

A. New Amazon SES users who have received production access can send up to 1,000 emails per 24-hour period, at a maximum rate of 10 emails per second.
B. Every Amazon SES sender has a the same set of sending limits
C. Sending limits are based on messages rather than on recipients
D. Every Amazon SES sender has a unique set of sending limits

Answer: D

Explanation:
Amazon Simple Email Service (Amazon SES) is a highly scalable and cost-effective email-sending
service for businesses and developers. Amazon SES eliminates the complexity and expense of building an in-house email solution or licensing, installing, and operating a third-party email service for this type of email communication.
Every Amazon SES sender has a unique set of sending limits, which are calculated by Amazon SES on an ongoing basis:
Sending quota — the maximum number of emails you can send in a 24-hour period. Maximum send rate — the maximum number of emails you can send per second.
New Amazon SES users who have received production access can send up to 10,000 emails per 24-hour period, at a maximum rate of 5 emails per second.
Amazon SES automatically adjusts these limits upward, as long as you send high-quality email. If your existing quota is not adequate for your needs and the system has not automatically increased your quota, you can submit an SES Sending Quota Increase case at any time.
Sending limits are based on recipients ratherthan on messages. You can check your sending limits at any time by using the Amazon SES console.
Note that if your email is detected to be of poor or QUESTION able quality (e.g., high complaint rates, high bounce rates, spam, or abusive content), Amazon SES might temporarily or permanently reduce your permitted send volume, or take other action as AWS deems appropriate.
Reference: https://aws.amazon.com/ses/faqs/

NEW QUESTION 162
A for a VPC is a collection of subnets (typically private) that you may want to designate for your backend RDS DB Instances.

A. DB Subnet Set
B. RDS Subnet Group
C. DB Subnet Group
D. DB Subnet Collection

Answer: C

Explanation:
DB Subnet Groups are a set of subnets (one per Availability Zone of a particular region) designed for your DB instances that reside in a VPC. They make easy to manage Multi-AZ deployments as well as the conversion from a Single-AZ to a Mut|i-AZ one.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSVPC.html

NEW QUESTION 167
Amazon Elastic Load Balancing is used to manage traffic on a fileet of Amazon EC2 instances, distributing traffic to instances across all availability zones within a region. Elastic Load Balancing has all the advantages of an on-premises load balancer, plus several security benefits.
Which of the following is not an advantage of ELB over an on-premise load balancer?

A. ELB uses a four-tier, key-based architecture for encryption.
B. ELB offers clients a single point of contact, and can also serve as the first line of defense against attacks on your network.
C. ELB takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer.
D. ELB supports end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections.

Answer: A

Explanation:
Amazon Elastic Load Balancing is used to manage traffic on a fileet of Amazon EC2 instances, distributing traffic to instances across all availability zones within a region. Elastic Load Balancing has all the advantages of an on-premises load balancer, plus several security benefits:
Takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer
Offers clients a single point of contact, and can also serve as the first line of defense against attacks on your network
When used in an Amazon VPC, supports creation and management of security groups associated with your Elastic Load Balancing to provide additional networking and security options

Supports end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections. When TLS is used, the TLS server certificate used to terminate client connections can be managed centrally on the load balancer, rather than on every indMdual instance. Reference: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

NEW QUESTION 169
You have set up an S3 bucket with a number of images in it and you have decided that you want anybody to be able to access these images, even anonymous users. To accomplish this you create a bucket policy. You will need to use an Amazon S3 bucket policy that specifies a in the principal element, which means anyone can access the bucket.

A. hash tag (#)
B. anonymous user
C. wildcard (*)
D. S3 user

Answer: C

Explanation:
You can use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket. You can then use the generated document to set your bucket policy by using the Amazon S3 console, by a number of third-party tools, or via your application.
You use an Amazon S3 bucket policy that specifies a wildcard (*) in the principal element, which means anyone can access the bucket. With anonymous access, anyone (including users without an AWS account) will be able to access the bucket.
Reference: http://docs.aws.amazon.com/IAM/|atest/UserGuide/iam-troubleshooting.htm|#d0e20565

NEW QUESTION 173
You have been asked to build AWS infrastructure for disaster recovery for your local applications and within that you should use an AWS Storage Gateway as part of the solution. Which of the following best describes the function of an AWS Storage Gateway?

A. Accelerates transferring large amounts of data between the AWS cloud and portable storage devices .
B. A web service that speeds up distribution of your static and dynamic web content.
C. Connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between your on-premises IT environment and AWS's storage infrastructure.
D. Is a storage service optimized for infrequently used data, or "cold data."

Answer: C

Explanation:
AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the Amazon Web Services (AWS) storage infrastructure. You can use the service to store data in the AWS cloud for scalable and cost-effective storage that helps maintain data security. AWS Storage Gateway offers both volume-based and tape-based storage solutions:
Volume gateways Gateway-cached volumes Gateway-stored volumes
Gateway-virtual tape library (VTL)
Reference:
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_disasterrecovery_07.pdf

NEW QUESTION 178
What is the time period with which metric data is sent to CIoudWatch when detailed monitoring is enabled on an Amazon EC2 instance?

A. 15 minutes
B. 5 minutes
C. 1 minute
D. 45 seconds

Answer: C

Explanation:
By default, Amazon EC2 metric data is automatically sent to CIoudWatch in 5-minute periods. However, you can, enable detailed monitoring on an Amazon EC2 instance, which sends data to CIoudWatch in
1-minute periods
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.htmI

NEW QUESTION 180
Which of the following features are provided by Amazon EC2?

A. Exadata Database Machine, Optimized Storage Management, Flashback Technology, and Data Warehousing
B. Instances, Amazon Machine Images (AMIs), Key Pairs, Amazon EBS Volumes, Firewall, Elastic IP address, Tags, and Virtual Private Clouds (VPCs)
C. Real Application Clusters (RAC), Elasticache Machine Images (EMIs), Data Warehousing, Flashback Technology, Dynamic IP address
D. Exadata Database Machine, Real Application Clusters (RAC), Data Guard, Table and Index Partitioning, and Data Pump Compression

Answer: B

Explanation:
Amazon EC2 provides the following features:
· Virtual computing environments, known as instances;
· Pre-configured templates for your instances, known as Amazon Nlachine Images (AMIs), that package the bits you need for your server (including the operating system and additional software)
· Various configurations of CPU, memory, storage, and networking capacity for your instances, known as instance types
· Secure login information for your instances using key pairs (AWS stores the public key, and you store the private key in a secure place)
· Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as instance store volumes
· Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as Amazon EBS volumes

· Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as regions and Availability Zones
· A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
· Static IP addresses for dynamic cloud computing, known as Elastic IP addresses
· Metadata, known as tags, that you can create and assign to your Amazon EC2 resources
· Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as virtual private clouds (VPCs).
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

NEW QUESTION 185
A friend tells you he is being charged $100 a month to host his WordPress website, and you tell him you can move it to AWS for him and he will only pay a fraction of that, which makes him very happy. He then tells you he is being charged $50 a month for the domain, which is registered with the same people that set it up, and he asks if it's possible to move that to AWS as well. You tell him you aren't sure, but will look into it. Which of the following statements is true in regards to transferring domain names to AWS?

A. You can't transfer existing domains to AWS.
B. You can transfer existing domains into Amazon Route 53's management.
C. You can transfer existing domains via AWS Direct Connect.
D. You can transfer existing domains via AWS Import/Expor

Answer: B

Explanation:
With Amazon Route 53, you can create and manage your public DNS records with the AWS Management Console or with an easy-to-use API. If you need a domain name, you can find an available name and register it using Amazon Route 53. You can also transfer existing domains into Amazon Route 53's management.
Reference: http://aws.amazon.com/route53/

NEW QUESTION 190
Are penetration tests allowed as long as they are limited to the customer's instances?

A. Yes, they are allowed but only for selected regions.
B. No, they are never allowed.
C. Yes, they are allowed without any permission.
D. Yes, they are allowed but only with approval.

Answer: D

Explanation:
Penetration tests are allowed after obtaining permission from AWS to perform them. Reference: http://aws.amazon.com/security/penetration-testing/

NEW QUESTION 191
A user has created an ELB with the availability zone US-East-1A. The user wants to add more zones to ELB to achieve High Availability. How can the user add more zones to the existing ELB?

A. The user should stop the ELB and add zones and instances as required
B. The only option is to launch instances in different zones and add to ELB
C. It is not possible to add more zones to the existing ELB
D. The user can add zones on the fly from the AWS console

Answer: D

Explanation:
The user has created an Elastic Load Balancer with the availability zone and wants to add more zones to the existing ELB. The user can do so in two ways:
From the console or CLI, add new zones to ELB;
Launch instances in a separate AZ and add instances to the existing ELB. Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/enable-disable-az.html

NEW QUESTION 196
AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. In addition to supporting IAM user policies, some services support resource-based permissions. Which of the following services are supported by resource-based permissions?

A. Amazon SNS, and Amazon SQS and AWS Direct Connect.
B. Amazon S3 and Amazon SQS and Amazon ElastiCache.
C. Amazon S3, Amazon SNS, Amazon SQS, Amazon Glacier and Amazon EBS.
D. Amazon Glacier, Amazon SNS, and Amazon CloudWatch

Answer: C

Explanation:
In addition to supporting IAM user policies, some services support resource-based permissions, which let you attach policies to the service's resources instead of to IAM users or groups. Resource-based permissions are supported by Amazon S3, Amazon SNS, Amazon SQS, Amazon Glacier and Amazon EBS.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SpecificProducts.htm|

NEW QUESTION 200
You are setting up your first Amazon Virtual Private Cloud (Amazon VPC) network so you decide you should probably use the AWS Management Console and the VPC Wizard. Which of the following is not an option for network architectures after launching the "Start VPC Wizard" in Amazon VPC page on the AWS Management Console?

A. VPC with a Single Public Subnet Only
B. VPC with a Public Subnet Only and Hardware VPN Access
C. VPC with Public and Private Subnets and Hardware VPN Access
D. VPC with a Private Subnet Only and Hardware VPN Access

Answer: B

Explanation:
Amazon VPC enables you to build a virtual network in the AWS cloud - no VPNs, hardware, or physical datacenters required.
Your AWS resources are automatically provisioned in a ready-to-use default VPC. You can choose to create additional VPCs by going to Amazon VPC page on the AWS Management Console and click on the "Start VPC Wizard" button.
You'll be presented with four basic options for network architectures. After selecting an option, you can modify the size and IP address range of the VPC and its subnets. If you select an option with Hardware VPN Access, you will need to specify the IP address of the VPN hardware on your network. You can modify the VPC to add more subnets or add or remove gateways at any time after the VPC has been created.
The four options are:
VPC with a Single Public Subnet Only VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access VPC with a Private Subnet Only and Hardware VPN Access Reference:
https://aws.amazon.com/vpc/faqs/

NEW QUESTION 204
A user is trying to launch a similar EC2 instance from an existing instance with the option "Launch More like this". The AMI ofthe selected instance is deleted. What will happen in this case?

A. AWS does not need an AMI for the "Launch more like this" option
B. AWS will launch the instance but will not create a new AMI
C. AWS will create a new AMI and launch the instance
D. AWS will throw an error saying that the AMI is deregistered

Answer: D

Explanation:
If the user has deregistered the AMI of an EC2 instance and is trying to launch a similar instance with the option "Launch more like this", AWS will throw an error saying that the AMI is deregistered or not available.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html

NEW QUESTION 206
You are architecting a highly-scalable and reliable web application which will have a huge amount of content .You have decided to use Cloudfront as you know it will speed up distribution of your static and dynamic web content and know that Amazon C|oudFront integrates with Amazon CIoudWatch metrics so that you can monitor your web application. Because you live in Sydney you have chosen the the Asia Pacific (Sydney) region in the AWS console. However you have set up this up but no CIoudFront metrics seem to be appearing in the CIoudWatch console. What is the most likely reason from the possible choices below for this?

A. Metrics for CIoudWatch are available only when you choose the same region as the application you aremonitoring.
B. You need to pay for CIoudWatch for it to become active.
C. Metrics for CIoudWatch are available only when you choose the US East (
D. Virginia)
E. Metrics for CIoudWatch are not available for the Asia Pacific region as ye

Answer: C

Explanation:
CIoudFront is a global service, and metrics are available only when you choose the US East (N. Virginia) region in the AWS console. If you choose another region, no CIoudFront metrics will appear in the CIoudWatch console.
Reference:
http://docs.aws.amazon.com/AmazonCIoudFront/latest/Deve|operGuide/monitoring-using-cloudwatch.ht ml

NEW QUESTION 211
In the most recent company meeting, your CEO focused on the fact that everyone in the organization needs to make sure that all of the infrastructure that is built is truly scalable. Which of the following statements is incorrect in reference to scalable architecture?

A. A scalable service is capable of handling heterogeneity.
B. A scalable service is resilient.
C. A scalable architecture won't be cost effective as it grows.
D. Increasing resources results in a proportional increase in performanc

Answer: C

Explanation:
In AWS it is critical to build a scalable architecture in order to take advantage of a scalable infrastructure. The cloud is designed to provide conceptually infinite scalability. However, you cannot leverage all that scalability in infrastructure if your architecture is not scalable. Both have to work together. You will have to identify the monolithic components and bottlenecks in your architecture, identify the areas where you cannot leverage the on-demand provisioning capabilities in your architecture, and work to refactor your application, in order to leverage the scalable infrastructure and take advantage of the cloud.
Characteristics of a truly scalable application:
Increasing resources results in a proportional increase in performance A scalable service is capable of handling heterogeneity
A scalable service is operationally efficient A scalable service is resilient
A scalable service should become more cost effective when it grows (Cost per unit reduces as the number of units increases)
Reference: http://media.amazonwebservices.com/AWS_CIoud_Best_Practices.pdf

NEW QUESTION 216
A user has defined an AutoScaling termination policy to first delete the instance with the nearest billing hour. AutoScaling has launched 3 instances in the US-

East-1A region and 2 instances in the US-East-1 B region. One of the instances in the US-East-1B region is running nearest to the billing hour. Which instance will AutoScaling terminate first while executing the termination action?

A. Random Instance from US-East-1A
B. Instance with the nearest billing hour in US-East-1 B
C. Instance with the nearest billing hour in US-East-1A
D. Random instance from US-East-1B

Answer: C

Explanation:
Even though the user has configured the termination policy, before AutoScaling selects an instance to terminate, it first identifies the Availability Zone that has more instances than the other Availability Zones used by the group. Within the selected Availability Zone, it identifies the instance that matches the specified termination policy.
Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/us-termination-policy.html

NEW QUESTION 218
In Route 53, what does a Hosted Zone refer to?

A. A hosted zone is a collection of geographical load balancing rules for Route 53.
B. A hosted zone is a collection of resource record sets hosted by Route 53.
C. A hosted zone is a selection of specific resource record sets hosted by CloudFront for distribution to Route 53.
D. A hosted zone is the Edge Location that hosts the Route 53 records for a use

Answer: B

Explanation:
A Hosted Zone refers to a selection of resource record sets hosted by Route 53.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHostedZones.html

NEW QUESTION 223
Which of the following statements is true of Amazon EC2 security groups?

A. You can change the outbound rules for EC2-Classi
B. Also, you can add and remove rules to a group at any time.
C. You can modify an existing rule in a grou
D. However, you can't add and remove rules to a group.
E. None of the statements are correct.
F. You can't change the outbound rules for EC2-Classi
G. However, you can add and remove rules to agroup at any tim

Answer: D

Explanation:
When dealing with security groups, bear in mind that you can freely add and remove rules from a group, but you can't change the outbound rules for EC2-Classic. If you're using the Amazon EC2 console, you can modify existing rules, and you can copy the rules from an existing security group to a new security group.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

NEW QUESTION 227
Which DNS name can only be resolved within Amazon EC2?

A. Public DNS name
B. Internal DNS name
C. External DNS name
D. Global DNS name

Answer: B

Explanation:
Only Internal DNS name can be resolved within Amazon EC2. Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-instance-addressing.html

NEW QUESTION 228
You need to create a management network using network interfaces for a virtual private cloud (VPC) network. Which of the following statements is incorrect pertaining to Best Practices for Configuring Network Interfaces.

A. You can detach secondary (ethN) network interfaces when the instance is running or stoppe
B. However, you can't detach the primary (eth0) interface.
C. Launching an instance with multiple network interfaces automatically configures interfaces, private IP addresses, and route tables on the operating system of the instance.
D. You can attach a network interface in one subnet to an instance in another subnet in the same VPC, however, both the network interface and the instance must reside in the same Availability Zone.
E. Attaching another network interface to an instance is a valid method to increase or double the network bandwidth to or from the dual-homed instance

Answer: D

Explanation:
Best Practices for Configuring Network Interfaces

You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).
You can detach secondary (ethN) network interfaces when the instance is running or stopped. However, you can't detach the primary (eth0) interface.
You can attach a network interface in one subnet to an instance in another subnet in the same VPC, however, both the network interface and the instance must reside in the same Availability Zone.
When launching an instance from the CLI or API, you can specify the network interfaces to attach to the instance for both the primary (eth0) and additional network interfaces.
Launching an instance with multiple network interfaces automatically configures interfaces, private IP addresses, and route tables on the operating system of the instance.
A warm or hot attach of an additional network interface may require you to manually bring up the second interface, configure the private IP address, and modify the route table accordingly. (Instances running Amazon Linux automatically recognize the warm or hot attach and configure themselves.)
Attaching another network interface to an instance is not a method to increase or double the network bandwidth to or from the dual-homed instance.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#use-network-and-security-applia nces-in-your-vpc

NEW QUESTION 231
Your manager has asked you to set up a public subnet with instances that can send and receive internet traffic, and a private subnet that can't receive traffic directly from the internet, but can initiate traffic to the internet (and receive responses) through a NAT instance in the public subnet. Hence, the following 3 rules need to be allowed:
Inbound SSH traffic.
Web sewers in the public subnet to read and write to MS SQL servers in the private subnet Inbound RDP traffic from the Microsoft Terminal Services gateway in the public private subnet What are the respective ports that need to be opened for this?

A. Ports 22,1433,3389
B. Ports 21,1433,3389
C. Ports 25,1433,3389
D. Ports 22,1343,3999

Answer: A

Explanation:
A network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.
The following ports are recommended by AWS for a single subnet with instances that can receive and send Internet traffic and a private subnet that can't receive traffic directly from the Internet. However, it can initiate traffic to the Internet (and receive responses) through a NAT instance in the public subnet. Inbound SSH traffic. Port 22
Web sewers in the public subnet to read and write to MS SQL sewers in the private subnet. Port 1433 Inbound RDP traffic from the Microsoft Terminal Sewices gateway in the public private subnet. Port 3389 Reference:
http://docs.aws.amazon.com/AmazonVPC/Iatest/UserGuide/VPC_Appendix_NACLs.htm|#VPC_Appendi x_NAC Ls_Scenario_2

NEW QUESTION 236
A user has launched an EC2 instance. The instance got terminated as soon as it was launched. Which of the below mentioned options is not a possible reason for this?

A. The user account has reached the maximum volume limit
B. The AM is missin
C. It is the required part
D. The snapshot is corrupt
E. The user account has reached the maximum EC2 instance limit

Answer: D

Explanation:
When the user account has reached the maximum number of EC2 instances, it will not be allowed to launch an instance. AWS will throw an 'Instance Limit Exceeded' error. For all other reasons, such as
"AMI is missing part", "Corrupt Snapshot" or "Volume limit has reached" it will launch an EC2 instance and then terminate it.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_|nstanceStraightToTerminated.html

NEW QUESTION 238
A user has created an ELB with Auto Scaling. Which of the below mentioned offerings from ELB helps the
user to stop sending new requests traffic from the load balancer to the EC2 instance when the instance is being deregistered while continuing in-flight requests?

A. ELB sticky session
B. ELB deregistration check
C. ELB auto registration Off
D. ELB connection draining

Answer: D

Explanation:
The Elastic Load Balancer connection draining feature causes the load balancer to stop sending new requests to the back-end instances when the instances are deregistering or become unhealthy, while ensuring that in-flight requests continue to be served.
Reference:
http://docs.aws.amazon.com/EIasticLoadBaIancing/latest/DeveIoperGuide/config-conn-drain.htmI

NEW QUESTION 240
While controlling access to Amazon EC2 resources, which of the following acts as a firewall that controls the traffic allowed to reach one or more instances?

A. A security group

B. An instance type
C. A storage cluster
D. An object

Answer: A

Explanation:
A security group acts as a firewall that controls the traffic allowed to reach one or more instances. When you launch an instance, you assign it one or more security groups.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

NEW QUESTION 244
Just when you thought you knew every possible storage option on AWS you hear someone mention Reduced Redundancy Storage (RRS) within Amazon S3. What is the ideal scenario to use Reduced Redundancy Storage (RRS)?

A. Huge volumes of data
B. Sensitve data
C. Non-critical or reproducible data
D. Critical data

Answer: C

Explanation:
Reduced Redundancy Storage (RRS) is a new storage option within Amazon S3 that enables customers to reduce their costs by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. RRS provides a lower cost, less durable, highly available storage option that is designed to sustain the loss of data in a single facility.
RRS is ideal for non-critical or reproducible data.
For example, RRS is a cost-effective solution for sharing media content that is durably stored elsewhere. RRS also makes sense if you are storing thumbnails and other resized images that can be easily reproduced from an original image.
Reference: https://aws.amazon.com/s3/faqs/

NEW QUESTION 246
Your manager has come to you saying that he is very confused about the bills he is receMng from AWS as he is getting different bills for every user and needs you to look into making it more understandable. Which of the following would be the best solution to meet his request?

A. AWS Billing Aggregation
B. Consolidated Billing
C. Deferred Billing
D. Aggregated Billing

Answer: B

Explanation:
Consolidated Billing enables you to consolidate payment for multiple AWS accounts within your company by designating a single paying account. Consolidated Billing enables you to see a combined view of AWS costs incurred by all accounts, as well as obtain a detailed cost report for each of the indMdual AWS accounts associated with your "Paying Account". Consolidated Billing is offered at no additional charge. Reference: https://aws.amazon.com/bi|Iing/faqs/

NEW QUESTION 248
A user is planning to host a mobile game on EC2 which sends notifications to active users on either high score or the addition of new features. The user should get this notification when he is online on his mobile device. Which of the below mentioned AWS services can help achieve this functionality?

A. AWS Simple Notification Service.
B. AWS Simple Email Service.
C. AWS Nlobile Communication Service.
D. AWS Simple Queue Service.

Answer: A

Explanation:
Amazon Simple Notification Service (Amazon SNS) is a fast, filexible, and fully managed push messaging service. Amazon SNS makes it simple and cost-effective to push to mobile devices, such as iPhone, iPad, Android, Kindle Fire, and internet connected smart devices, as well as pushing to other distributed services.
Reference: http://aws.amazon.com/sns

NEW QUESTION 249
Which one of the following can't be used as an origin server with Amazon CIoudFront?

A. A web server running in your infrastructure
B. Amazon S3
C. Amazon Glacier
D. A web server running on Amazon EC2 instances

Answer: C

Explanation:
Amazon CIoudFront is designed to work with Amazon S3 as your origin server, customers can also use Amazon C|oudFront with origin sewers running on Amazon EC2 instances or with any other custom origin.
Reference: http://docs.aws.amazon.com/AmazonCIoudFront/latest/DeveIoperGuide/distribution-web.html

NEW QUESTION 252
You have been asked to set up monitoring of your network and you have decided that Cloudwatch would be the best service to use. Amazon CIoudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CIoudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. Which of the following items listed can AWS Cloudwatch monitor?

A. Log files your applications generate.
B. All of the items listed on this page.
C. System-wide visibility into resource utilization, application performance, and operational health.
D. Custom metrics generated by your applications and services .

Answer: B

Explanation:
Amazon CIoudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CIoudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.
Reference: http://aws.amazon.com/cIoudwatch/

NEW QUESTION 257
After deciding that EMR will be useful in analysing vast amounts of data for a gaming website that you are architecting you have just deployed an Amazon EMR Cluster and wish to monitor the cluster performance. Which of the following tools cannot be used to monitor the cluster performance?

A. Kinesis
B. Ganglia
C. C|oudWatch Metrics
D. Hadoop Web Interfaces

Answer: A

Explanation:
Amazon EMR provides several tools to monitor the performance of your cluster. Hadoop Web Interfaces
Every cluster publishes a set of web interfaces on the master node that contain information about the cluster. You can access these web pages by using an SSH tunnel to connect them on the master node. For more information, see View Web Interfaces Hosted on Amazon EMR Clusters.
CIoudWatch Metrics
Every cluster reports metrics to CIoudWatch. CIoudWatch is a web service that tracks metrics, and which you can use to set alarms on those metrics. For more information, see Monitor Metrics with CIoudWatch. Ganglia
Ganglia is a cluster monitoring tool. To have this available, you have to install Ganglia on the cluster when you launch it. After you've done so, you can monitor the cluster as it runs by using an SSH tunnel to connect to the Ganglia UI running on the master node. For more information, see Monitor Performance with Ganglia.
Reference:
http://docs.aws.amazon.com/EIasticMapReduce/latest/DeveIoperGuide/emr-troubleshoot-tooIs.htmI

NEW QUESTION 258
Can you move a Reserved Instance from one Availability Zone to another?

A. Yes, but each Reserved Instance is associated with a specific Region that cannot be changed.
B. Yes, only in US-West-2.
C. Yes, only in US-East-1.
D. No

Answer: A

Explanation:
Each Reserved Instance is associated with a specific Region, which is fixed for the lifetime of the reservation and cannot be changed. Each reservation can, however, be used in any of the available AZs within the associated Region.
Reference: https://aws.amazon.com/rds/faqs/

NEW QUESTION 262
When controlling access to Amazon EC2 resources, each Amazon EBS Snapshot has a attribute that controls which AWS accounts can use the snapshot.

A. createVoIumePermission
B. LaunchPermission
C. SharePermission
D. RequestPermission

Answer: A

Explanation:
Each Amazon EBS Snapshot has a createVoIumePermission attribute that you can set to one or more AWS Account IDs to share the AM with those AWS Accounts. To allow several AWS Accounts to use a particular EBS snapshot, you can use the snapshots's createVoIumePermission attribute to include a list of the accounts that can use it.
Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM.html

NEW QUESTION 266
A 3-tier e-commerce web application is current deployed on-premises and will be migrated to AWS for
greater scalability and elasticity The web server currently shares read-only data using a network distributed file system The app server tier uses a clustering mechanism for discovery and shared session state that depends on I P multicast The database tier uses shared-storage clustering to provide database fail over capability, and uses several read slaves for scaling Data on all sewers and the distributed file system directory is backed up weekly to off-site tapes
Which AWS storage and database architecture meets the requirements of the application?

A. Web sewers: store read-only data in 53, and copy from 53 to root volume at boot tim
B. App servers: share state using a combination of DynamoDB and IP unicas
C. Database: use RDS with multi-AZ deployment and one or more read replica
D. Backup: web servers, app servers, and database backed up weekly to Glacier using snapshots.
E. Web sewers: store read-only data in an EC2 NFS server, mount to each web server at boot tim
F. App servers: share state using a combination of DynamoDB and IP multicas
G. Database: use RDS with multi-AZ deployment and one or more Read Replica
H. Backup: web and app servers backed up weekly via AM Is, database backed up via DB snapshots.
I. Web servers: store read-only data in 53, and copy from 53 to root volume at boot tim
J. App servers: share state using a combination of DynamoDB and IP unicas
K. Database: use RDS with multi-AZ deployment and one or more Read Replica
L. Backup: web and app servers backed up weekly viaAM Is, database backed up via DB snapshots.
M. Web servers: store read-only data in 53, and copy from 53 to root volume at boot tim
N. App servers: share state using a combination of DynamoDB and IP unicas
O. Database: use RDS with multi-AZ deploymen
P. Backup: web and app sewers backed up weekly via ANI Is, database backed up via DB snapshots.

Answer: C

Explanation:
Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure (for example, instance hardware failure, storage failure, or network disruption), Amazon RDS performs an automatic failover to the standby, so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.
Benefits
Enhanced Durability
MuIti-AZ deployments for the MySQL, Oracle, and PostgreSQL engines utilize synchronous physical replication to keep data on the standby up-to-date with the primary. MuIti-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL
Server-native Mrroring technology. Both approaches safeguard your data in the event of a DB Instance failure or loss of an Availability Zone.
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. Compare this to a Single-AZ deployment: in case of a Single-AZ database failure, a user-initiated point-in-time-restore operation will be required. This operation can take several hours to complete, and any data updates that occurred after the latest restorable time (typically within the last five minutes) will not be available.
Amazon Aurora employs a highly durable, SSD-backed virtualized storage layer purpose-built for
database workloads. Amazon Aurora automatically replicates your volume six ways, across three Availability Zones. Amazon Aurora storage is fault-tolerant, transparently handling the loss of up to two copies of data without affecting database write availability and up to three copies without affecting read availability. Amazon Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and replaced automatically.
Increased Availability
You also benefit from enhanced database availability when running Multi-AZ deployments. If an Availability Zone failure or DB Instance failure occurs, your availability impact is limited to the time automatic failover takes to complete: typically under one minute for Amazon Aurora and one to two minutes for other database engines (see the RDS FAQ for details).
The availability benefits of MuIti-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 fail over to complete.
Unlike Single-AZ deployments, 1/0 actMty is not suspended on your primary during backup for MuIti-AZ deployments for the MySOL, Oracle, and PostgreSQL engines, because the backup is taken from the standby. However, note that you may still experience elevated latencies for a few minutes during backups for Mu|ti-AZ deployments.
On instance failure in Amazon Aurora deployments, Amazon RDS uses RDS MuIti-AZ technology to automate failover to one of up to 15 Amazon Aurora Replicas you have created in any of three Availability Zones. If no Amazon Aurora Replicas have been provisioned, in the case of a failure, Amazon RDS will attempt to create a new Amazon Aurora DB instance for you automatically.
No Administrative Intervention
DB Instance failover is fully automatic and requires no administrative intervention. Amazon RDS monitors the health of your primary and standbys, and initiates a failover automatically in response to a variety of failure conditions.
Failover conditions
Amazon RDS detects and automatically recovers from the most common failure scenarios for Multi-AZ deployments so that you can resume database operations as quickly as possible without administrative intervention. Amazon RDS automatically performs a failover in the event of any of the following:
Loss of availability in primary Availability Zone Loss of network connectMty to primary Compute unit failure on primary
Storage failure on primary
Note: When operations such as DB Instance scaling or system upgrades like OS patching are initiated for Multi-AZ deployments, for enhanced availability, they are applied first on the standby prior to an automatic failover. As a result, your availability impact is limited only to the time required for automatic failover to complete.
Note that Amazon RDS Multi-AZ deployments do not failover automatically in response to database operations such as long running queries, deadlocks or database corruption errors.

NEW QUESTION 269
Your customer wishes to deploy an enterprise application to AWS which will consist of several web servers, several application servers and a small (50GB) Oracle database information is stored, both in the database and the file systems of the various servers. The backup system must support database recovery whole server and whole disk restores, and indMdual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database
Which backup architecture will meet these requirements?

A. Backup RDS using automated daily DB backups Backup the EC2 instances using AMs andsupplement with file-level backup to 53 using traditional enterprise backup software to provide fi Ie level restore
B. Backup RDS using a Multi-AZ Deployment Backup the EC2 instances using Amis, and supplement by copying file system data to 53 to provide file level restore.
C. Backup RDS using automated daily DB backups Backup the EC2 instances using EBS snapshots and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore
D. Backup RDS database to 53 using Oracle RMAN Backup the EC2 instances using Amis, and supplement with EBS snapshots for indMdual volume restore.

Answer: A

Explanation:
Point-In-Time Recovery
In addition to the daily automated backup, Amazon RDS archives database change logs. This enables you to recover your database to any point in time during the

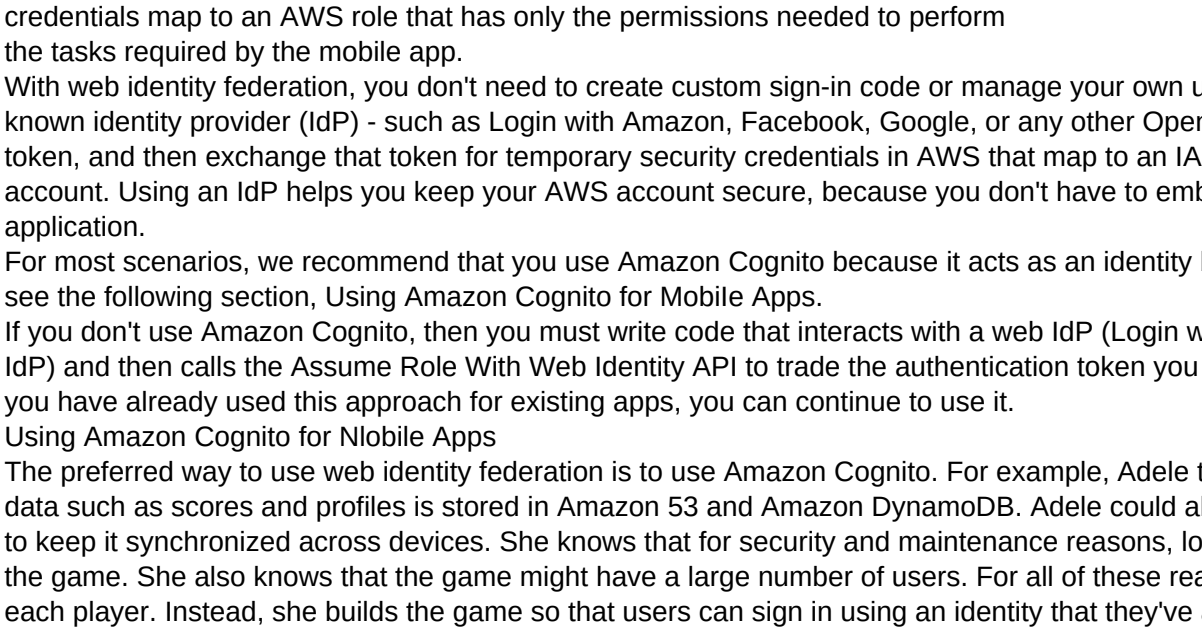
backup retention period, up to the last five minutes of database usage.
Amazon RDS stores multiple copies of your data, but for Single-AZ DB instances these copies are stored in a single availability zone. If for any reason a Single-AZ DB instance becomes unusable, you can use point-in-time recovery to launch a new DB instance with the latest restorable data. For more information on working with point-in-time recovery, go to Restoring a DB Instance to a Specified Time.
Note
Mu|ti-AZ deployments store copies of your data in different Availability Zones for greater levels of data durability. For more information on Multi-AZ deployments, see High Availability (MuIti-AZ).

NEW QUESTION 273
Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account to streamline data capture. Company B would like to directly save player data and scoring information from the mobile app to a DynamoDS table named Score Data
When a user saves their game the progress data will be stored to the Game state 53 bucket. What is the best approach for storing data to DynamoDB and 53?

A. Use an EC2 Instance that is launched with an EC2 role providing access to the Score Data DynamoDB table and the GameState 53 bucket that communicates with the mobile app via web services.
B. Use temporary security credentials that assume a role providing access to the Score Data DynamoDB table and the Game State 53 bucket using web identity federation.
C. Use Login with Amazon allowing users to sign in with an Amazon account providing the mobile app with access to the Score Data DynamoDB table and the Game State 53 bucket.
D. Use an IAM user with access credentials assigned a role providing access to the Score Data DynamoDB table and the Game State 53 bucket for distribution with the mobile app.

Answer: B

Explanation:
Web Identity Federation
Imagine that you are creating a mobile app that accesses AWS resources, such as a game that runs on a mobile device and stores player and score information using Amazon 53 and DynamoDB. When you write such an app, you'II 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.
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. Using an IdP helps you keep your AWS account secure, because you don't have to embed and distribute longterm security credentials with your application.
For most scenarios, we recommend that you use Amazon Cognito because it acts as an identity broker and does much of the federation work for you. For details, see the following section, Using Amazon Cognito for MobiIe Apps.
If you don't use Amazon Cognito, then you must write code that interacts with a web IdP (Login with Amazon, Facebook, Google, or any other OIDC-compatible IdP) and then calls the Assume Role With Web Identity API to trade the authentication token you get from those IdPs for AWS temporary security credentials. If you have already used this approach for existing apps, you can continue to use it.
Using Amazon Cognito for Nlobile Apps
The preferred way to use web identity federation is to use Amazon Cognito. For example, Adele the developer is building a game for a mobile device where user data such as scores and profiles is stored in Amazon 53 and Amazon DynamoDB. Adele could also store this data locally on the device and use Amazon Cognito to keep it synchronized across devices. She knows that for security and maintenance reasons, long-term AWS security credentials should not be distributed with the game. She also knows that the game might have a large number of users. For all of these reasons, she does not want to create new user identities in IAM for each player. Instead, she builds the game so that users can sign in using an identity that they've already established with a well-known identity provider, such as Login with Amazon, Facebook, Google, or any OpenID Connect {OIDC)-compatible identity provider.
Her game can take advantage of the authentication mechanism from one of these providers to validate the user's identity.
To enable the mobile app to access her AWS resources, Adele first registers for a developer 10 with her chosen IdPs. She also configures the application with each of these providers. In her AWS account that contains the Amazon 53 bucket and DynamoDB table for the game, Adele uses Amazon Cognito to create IAM roles that precisely define permissions that the game needs. If she is using an OIDC IdP, she also creates an IAM OIDC identity provider entity to establish t rust between her AWS account and the IdP.
In the app's code, Adele calls the sign-in interface for the IdP that she configured previously. The IdP handles all the details of letting the user sign in, and the app gets an OAuth access token or OIDC ID token from the provider. AdeIe's app can trade this authentication information for a set of temporary security credentials that consist of an AWS access key 10, a secret access key, and a session token.
The app can then use these credentials to access web services offered by AWS. The app is limited to the permissions that are defined in the role that it assumes.
The following figure shows a simplified flow for how this might work, using Login with Amazon as the IdP.
For Step 2, the app can also use Facebook, Google, or any OIDC-compatible identity provider, but that's not shown here.
Sample workflow using Amazon Cognito to federate users for a mobile application



A customer starts your app on a mobile device. The app asks the user to sign in. The app uses Login with Amazon resources to accept the user's credentials.
The app uses Cognito APIs to exchange the Login with Amazon 10 token for a Cognito token. The app requests temporary security credentials from AWS STS, passing the Cognito token.
The temporary security credentials can be used by the app to access any AWS resources required by the app to operate. The role associated with the temporary

security credentials and its assigned policies determines what can be accessed.
Use the following process to configure your app to use Amazon Cognito to authenticate users and give your app access to AWS resources. For specific steps to accomplish this scenario, consult the documentation for Amazon Cognito.
(Optional) Sign up as a developer with Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC}-compatible identity provider and configure one or more apps with the provider. This step is optional because Amazon Cognito also supports unauthenticated (guest) access for your users.
Go to Amazon Cognito in the AWS IV|anagement Console. Use the Amazon Cognito wizard to create an identity pool, which is a container that Amazon Cognito uses to keep end user identities organized for your apps. You can share identity pools between apps. When you set up an identity pool, Amazon Cognito creates one or two IAM roles (one for authenticated identities, and one for unauthenticated "guest" identities) that define permissions for Amazon Cognito users.
Download and integrate the AWS SDK for iOS or the AWS SDK for Android with your app, and import the files required to use Amazon Cognito.
Create an instance of the Amazon Cognito credentials provider, passing the identity pool ID, your AWS account number, and the Amazon Resource Name (ARN) of the ro les that you associated with the identity pool. The Amazon Cognito wizard in the AWS Management Console provides sample code to help you get started.
When your app accesses an AWS resource, pass the credentials provider instance to the client object, which passes temporary security credentials to the client. The permissions for the credentials are based on the role or roles that you defined earlier.

NEW QUESTION 275
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AWS-Solution-Architect-Associate Practice Exam Features:

* AWS-Solution-Architect-Associate Questions and Answers Updated Frequently

* AWS-Solution-Architect-Associate Practice Questions Verified by Expert Senior Certified Staff

* AWS-Solution-Architect-Associate Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Solution-Architect-Associate Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year