AWS Certified Solutions Architect - Professional.VCEup.com.May-2022.468q

Number: Architect-Prof
Passing Score: 800
Time Limit: 120 min

AWS-Architect

AWS Certified Solutions Architect – Professional

Exam A

QUESTION 1
Your company policies require encryption of sensitive data at rest. You are considering the possible options for protecting data while storing it at rest on an EBS data volume, attached to an EC2 instance.

Which of these options would allow you to encrypt your data at rest? (Choose 3)

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A customer is deploying an SSL enabled web application to AWS and would like to implement a separation of roles between the EC2 service administrators that are entitled to login to instances as well as making API calls and the security officers who will maintain and have exclusive access to the application's X.509 certificate that contains the private key.

A. Upload the certificate on an S3 bucket owned by the security officers and accessible only by EC2 Role of the web servers.
B. Configure the web servers to retrieve the certificate upon boot from an CloudHSM is managed by the security officers.
C. Configure system permissions on the web servers to restrict access to the certificate only to the authority security officersD. Configure IAM policies authorizing access to the certificate store only to the security officers and terminate SSL on an ELB.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You'll terminate the SSL at ELB. and the web request will get unencrypted to the EC2 instance, even if the certs are stored in S3, it has to be configured on the web servers or load balancers somehow, which becomes difficult if the keys are stored in S3. However, keeping the keys in the cert store and using IAM to restrict access gives a clear separation of concern between security officers and developers. Developer's personnel can still configure SSL on ELB without actually handling the keys.

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

Which setup win meet the requirements?

A. Add an SQS queue to the ingestion layer to buffer writes to the RDS instance
B. Ingest data into a DynamoDB table and move old data to a Redshift cluster
C. Replace the RDS instance with a 6 node Redshift cluster with 96TB of storage
D. Keep the current architecture but upgrade RDS storage to 3TB and 10K provisioned IOPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The POC solution is being scaled up by 1000, which means it will require 72TB of Storage to retain 24 months' worth of data. This rules out RDS as a possible DB solution which leaves you with Redshift. I believe DynamoDB is a more cost effective and scales better for ingest rather than using EC2 in an auto scaling group.
Also, this example solution from AWS is somewhat similar for reference.
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_timeseriesprocessing_16.pdf

QUESTION 4 A web company is looking to implement an intrusion detection and prevention system into their deployed VPC. This platform should have the ability to scale to thousands of instances running inside of the VPC.

How should they architect their solution to achieve these goals?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A company is storing data on Amazon Simple Storage Service (S3). The company's security policy mandates that data is encrypted at rest.

Which of the following methods can achieve this? (Choose 3)

A. Use Amazon S3 server-side encryption with AWS Key Management Service managed keys.
B. Use Amazon S3 server-side encryption with customer-provided keys.
C. Use Amazon S3 server-side encryption with EC2 key pair.
D. Use Amazon S3 bucket policies to restrict access to the data at rest.
E. Encrypt the data on the client-side before ingesting to Amazon S3 using their own master key.
F. Use SSL to encrypt the data while in transit to Amazon S3.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

QUESTION 6
Your firm has uploaded a large amount of aerial image data to S3. In the past, in your on-premises environment, you used a dedicated group of servers to oaten process this data and used Rabbit MQ - An open source messaging system to get job information to the servers. Once processed the data would go to tape and be shipped offsite. Your manager told you to stay with the current design, and leverage AWS archival storage and messaging services to minimize cost.

Which is correct?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You've been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3. They are using a combination of RDS and DynamoOB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and suspect someone is attempting to gain unauthorized access.

Which approach provides a cost effective scalable mitigation to this kind of attack?

A. Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC they would then establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF). And then pass the traffic through the DirectConnect connection into their application running in their VPC. B. Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
C. Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would their pass the traffic to the currentweb tier The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group
D. Remove all but TLS 1.2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Your company is in the process of developing a next generation pet collar that collects biometric information to assist families with promoting healthy lifestyles for their pets. Each collar will push 30kb of biometric data in JSON format every 2 seconds to a collection platform that will process and analyze the data providing health trending information back to the pet owners and veterinarians via a web portal. Management has tasked you to architect the collection platform ensuring the following requirements are met.

▪ Provide the ability for real-time analytics of the inbound biometric data
▪ Ensure processing of the biometric data is highly durable. Elastic and parallel ▪
The results of the analytic processing should be persisted for data mining

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
You are designing Internet connectivity for your VPC. The Web servers must be available on the Internet. The application must have a highly available architecture.

Which alternatives should you consider? (Choose 2)

A. Configure a NAT instance in your VPC. Create a default route via the NAT instance and associate it with all subnets. Configure a DNS A record that points to the NAT instance public IP address.
B. Configure a CloudFront distribution and configure the origin to point to the private IP addresses of your Web servers. Configure a Route53 CNAME record to your CloudFront distribution.
C. Place all your web servers behind ELB. Configure a Route53 CNMIE to point to the ELB DNS name.
D. Assign EIPs to all web servers. Configure a Route53 record set with all EIPs, with health checks and DNS failover.
E. Configure ELB with an EIP. Place all your Web servers behind ELB. Configure a Route53 A record that points to the EIP.
Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Your team has a tomcat-based Java application you need to deploy into development, test and production environments. After some research, you opt to use Elastic Beanstalk due to its tight integration with your developer tools and RDS due to its ease of management. Your QA team lead points out that you need to roll a sanitized set of production data into your environment on a nightly basis. Similarly, other software teams in your org want access to that same restored data via their EC2 instances in your VPC.

The optimal setup for persistence and security that meets the above requirements would be the following.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Your company has an on-premises multi-tier PHP web application, which recently experienced downtime due to a large burst in web traffic due to a company announcement Over the coming days, you are expecting similar announcements to drive similar unpredictable bursts, and are looking to find ways to quickly improve your infrastructures ability to handle unexpected increases in traffic.
The application currently consists of 2 tiers a web tier which consists of a load balancer and several Linux Apache web servers as well as a database tier which hosts a Linux server hosting a MySQL database.

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

A. Failover environment: Create an S3 bucket and configure it for website hosting. Migrate your DNS to Route53 using zone file import, and leverage Route53 DNS failover to failover to the S3 hosted website.
B. Hybrid environment: Create an AMI, which can be used to launch web servers in EC2. Create an Auto Scaling group, which uses the AMI to scale the web tier based on incoming traffic. Leverage Elastic Load Balancing to balance trafficbetween on-premises web servers and those hosted in AWS.
C. Offload traffic from on-premises environment: Setup a CIoudFront distribution, and configure CloudFront to cache objects from a custom origin. Choose to customize your object cache behavior, and select a TTL that objects should existin cache.
D. Migrate to AWS: Use VM Import/Export to quickly convert an on-premises web server to an AMI. Create an Auto Scaling group, which uses the imported AMI to scale the web tier based on incoming traffic. Create an RDS read replicaand setup replication between the RDS instance and on-premises MySQL server to migrate the database.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
You are implementing AWS Direct Connect. You intend to use AWS public service end points such as Amazon S3, across the AWS Direct Connect link. You want other Internet traffic to use your existing link to an Internet Service Provider.

What is the correct way to configure AWS Direct connect for access to services such as Amazon S3?

A. Configure a public Interface on your AWS Direct Connect link. Configure a static route via your AWS Direct Connect link that points to Amazon S3 Advertise a default route to AWS using BGP.
B. Create a private interface on your AWS Direct Connect link. Configure a static route via your AWS Direct connect link that points to Amazon S3 Configure specific routes to your network in your VPC.
C. Create a public interface on your AWS Direct Connect link. Redistribute BGP routes into your existing routing infrastructure; advertise specific routes for your network to AWS.
D. Create a private interface on your AWS Direct connect link. Redistribute BGP routes into your existing routing infrastructure and advertise a default route to AWS.
Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

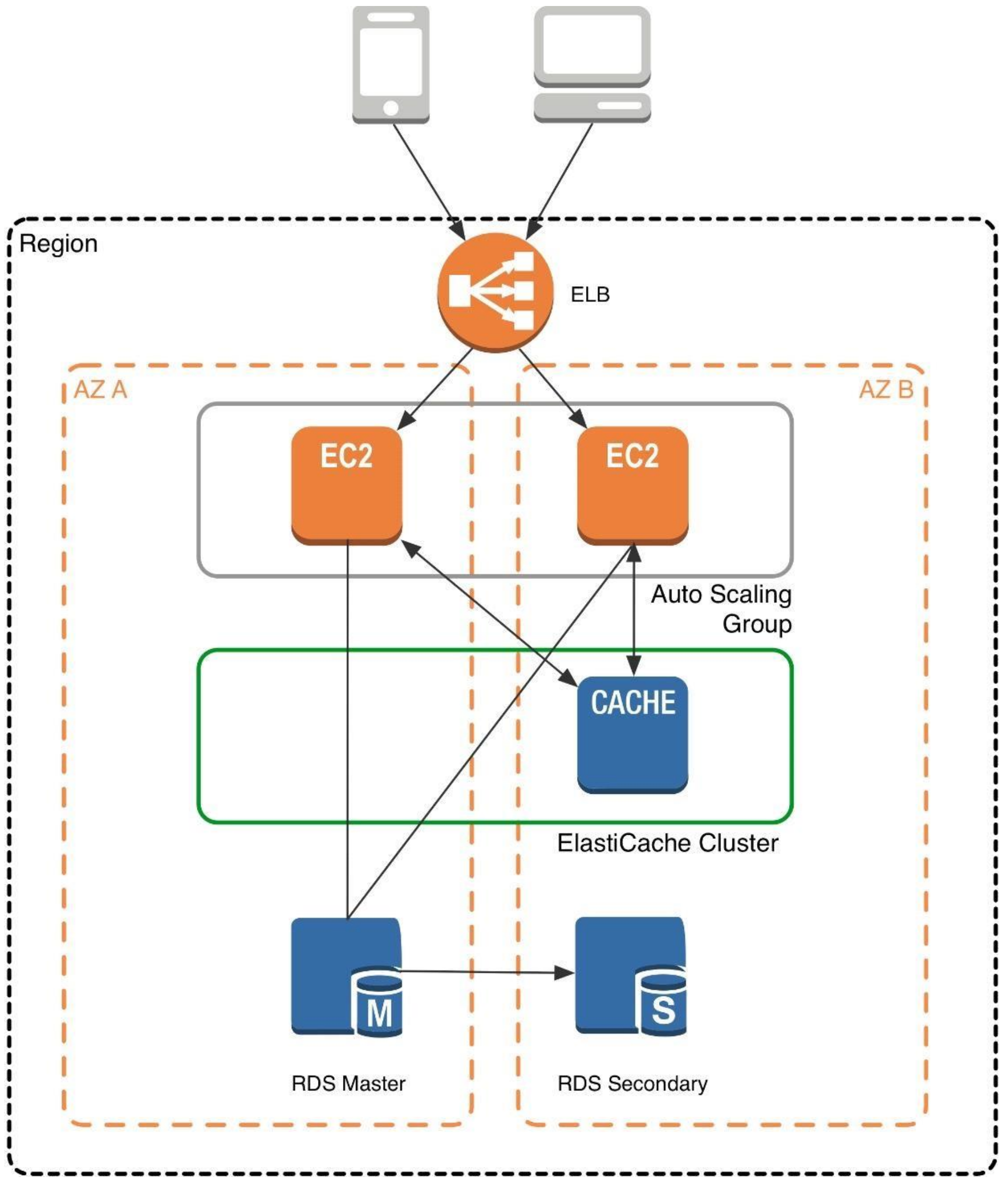
QUESTION 13
Your application is using an ELB in front of an Auto Scaling group of web/application servers deployed across two AZs and a Multi-AZ RDS Instance for data persistence.
The database CPU is often above 80% usage and 90% of I/O operations on the database are reads. To improve performance you recently added a single-node Memcached ElastiCache Cluster to cache frequent DB query results. In the next weeks the overall workload is expected to grow by 30%.

Do you need to change anything in the architecture to maintain the high availability or the application with the anticipated additional load? Why?

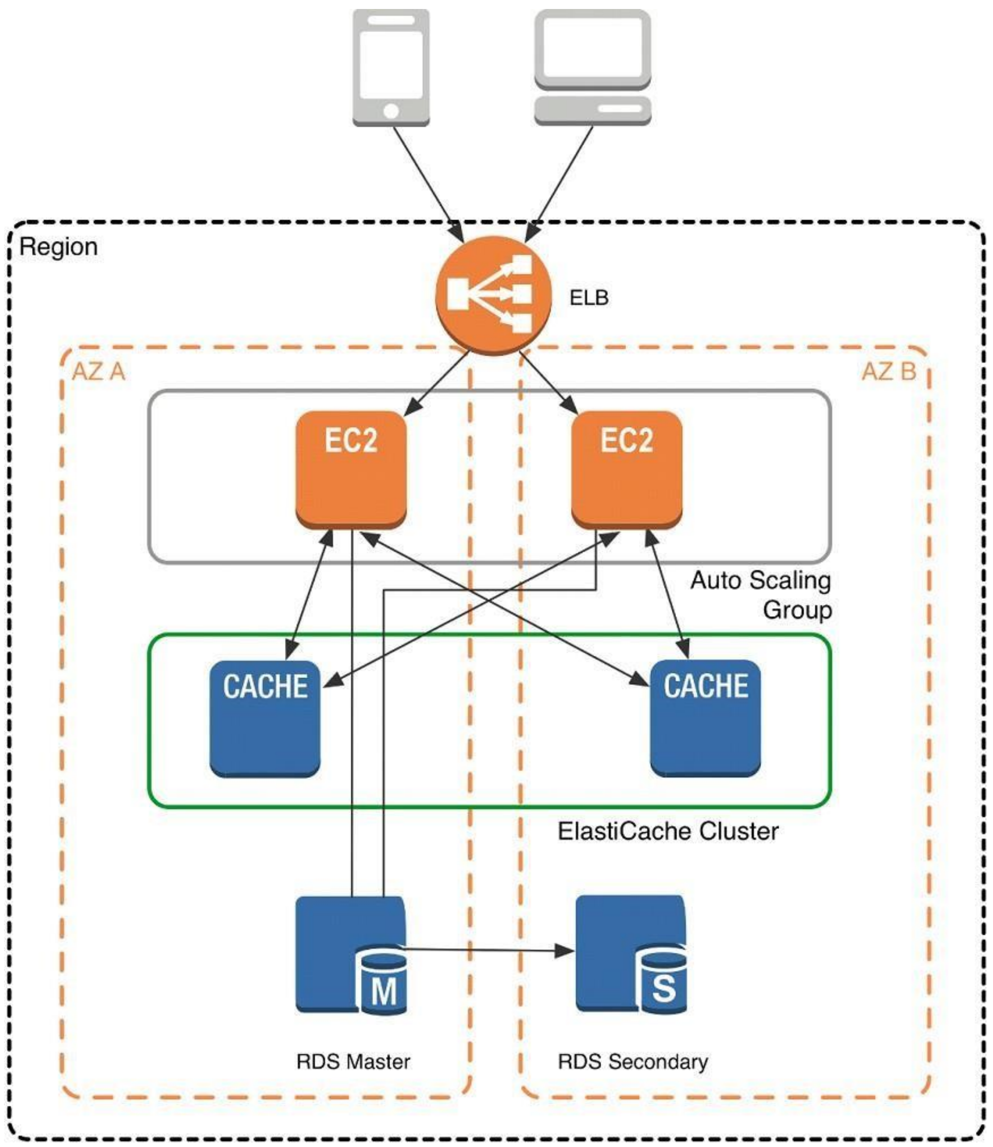
A. Yes, you should deploy two Memcached ElastiCache Clusters in different AZs because the RDS instance will not be able to handle the load if the cache node fails.
B. No, if the cache node fails you can always get the same data from the DB without having any availability impact.
C. No, if the cache node fails the automated ElastiCache node recovery feature will prevent any availability impact.
D. Yes, you should deploy the Memcached ElastiCache Cluster with two nodes in the same AZ as the RDS DB master instance to handle the load if one cache node fails.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ElastiCache for Memcached
The primary goal of caching is typically to offload reads from your database or other primary data source. In most apps, you have hot spots of data that are regularly queried, but only updated periodically. Think of the front page of a blog or news site, or the top 100 leaderboard in an online game. In this type of case, your app can receive dozens, hundreds, or even thousands of requests for the same data before it's updated again. Having your caching layer handle these queries has several advantages. First, it's considerably cheaper to add an in-memory cache than to scale up to a larger database cluster. Second, an in-memory cache is also easier to scale out, because it's easier to distribute an inmemory cache horizontally than a relational database.
Last, a caching layer provides a request buffer in the event of a sudden spike in usage. If your app or game ends up on the front page of Reddit or the App Store, it's not unheard of to see a spike that is 10 to 100 times your normal application load. Even if you autoscale your application instances, a 10x request spike will likely make your database very unhappy.
Let's focus on ElastiCache for Memcached first, because it is the best fit for a cachingfocused solution. We'll revisit Redis later in the paper, and weigh its advantages and disadvantages.
Architecture with ElastiCache for Memcached
When you deploy an ElastiCache Memcached cluster, it sits in your application as a separate tier alongside your database. As mentioned previously, Amazon ElastiCache does not directly communicate with your database tier, or indeed have any particular knowledge of your database. A simplified deployment for a web application looks something like this:

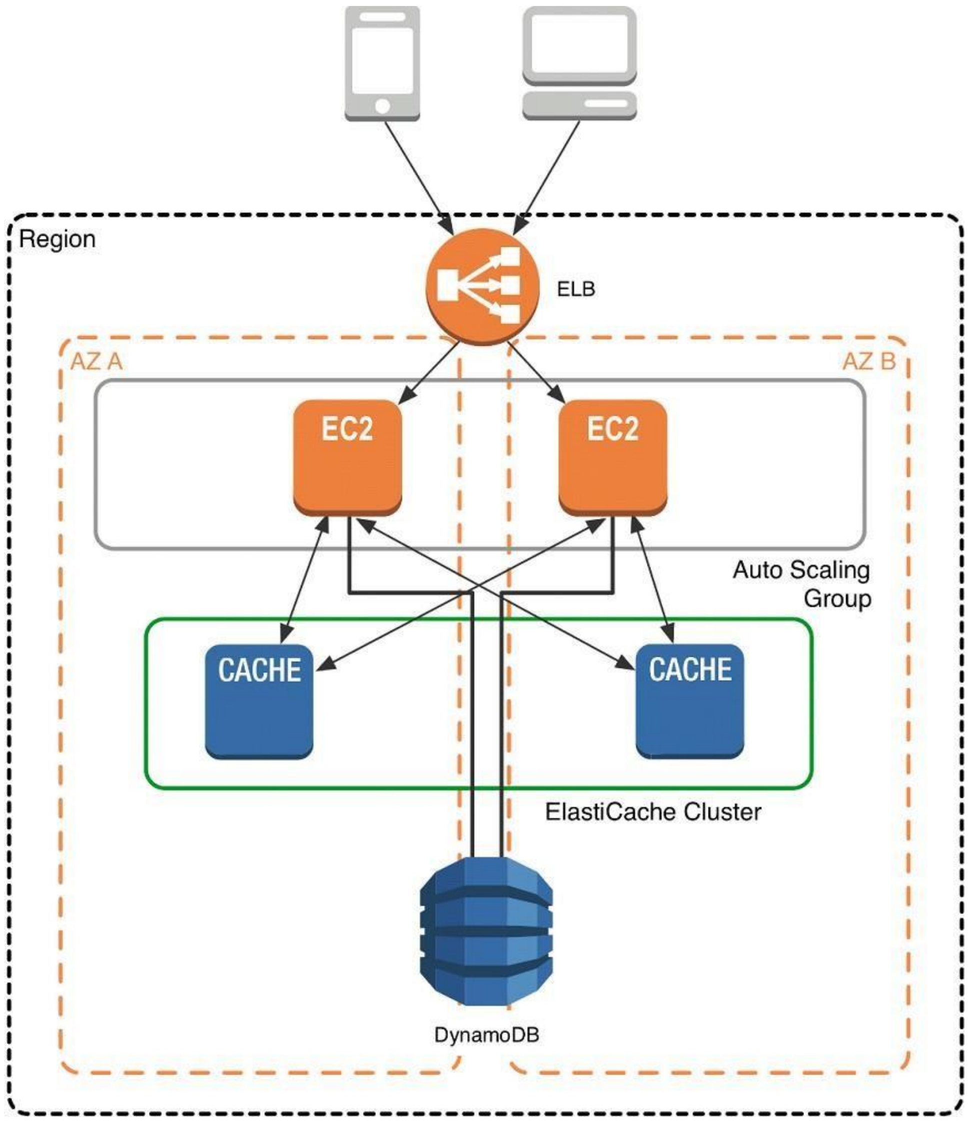


In this architecture diagram, the Amazon EC2 application instances are in an Auto Scaling group, located behind a load balancer using Elastic Load Balancing, which distributes requests among the instances. As requests come into a given EC2 instance, that EC2 instance is responsible for communicating with ElastiCache and the database tier. For development purposes, you can begin with a single ElastiCache node to test your application, and then scale to additional cluster nodes by modifying the ElastiCache cluster. As you add additional cache nodes, the EC2 application instances are able to distribute cache keys across multiple ElastiCache nodes. The most common practice is to use client-side sharding to distribute keys across cache nodes, which we will discuss later in this paper.



When you launch an ElastiCache cluster, you can choose the Availability Zone(s) that the cluster lives in. For best performance, you should configure your cluster to use the same Availability Zones as your application servers. To launch an ElastiCache cluster in a specific Availability Zone, make sure to specify the Preferred Zone(s) option during cache cluster creation. The Availability Zones that you specify will be where ElastiCache will launch your cache nodes. We recommend that you select Spread Nodes Across Zones, which tells ElastiCache to distribute cache nodes across these zones as evenly as possible. This distribution will mitigate the impact of an Availability Zone disruption on your ElastiCache nodes. The trade-off is that some of the requests from your application to ElastiCache will go to a node in a different Availability Zone, meaning latency will be slightly higher. For more details, refer to Creating a Cache Cluster in the Amazon ElastiCache User Guide.

As mentioned at the outset, ElastiCache can be coupled with a wide variety of databases. Here is an example architecture that uses Amazon DynamoDB instead of Amazon RDS and MySQL:



This combination of DynamoDB and ElastiCache is very popular with mobile and game companies, because DynamoDB allows for higher write throughput at lower cost than traditional relational databases. In addition, DynamoDB uses a key-value access pattern similar to ElastiCache, which also simplifies the programming model. Instead of using relational SQL for the primary database but then key-value patterns for the cache, both the primary database and cache can be programmed similarly. In this architecture pattern, DynamoDB remains the source of truth for data, but application reads are offloaded to ElastiCache for a speed boost.

QUESTION 14

An ERP application is deployed across multiple AZs in a single region. In the event of failure, the Recovery Time Objective (RTO) must be less than 3 hours, and the Recovery Point Objective (RPO) must be 15 minutes. The customer realizes that data corruption occurred roughly 1.5 hours ago.

What DR strategy could be used to achieve this RTO and RPO in the event of this kind of failure?

A. Take hourly DB backups to S3, with transaction logs stored in S3 every 5 minutes.
B. Use synchronous database master-slave replication between two availability zones.
C. Take hourly DB backups to EC2 Instance store volumes with transaction logs stored In S3 every 5 minutes.
D. Take 15 minute DB backups stored In Glacier with transaction logs stored in S3 every 5 minutes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

You are designing the network infrastructure for an application server in Amazon VPC. Users will access all application instances from the Internet, as well as from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link.

How would you design routing to meet the above requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 You control access to S3 buckets and objects with:

A. Identity and Access Management (IAM) Policies.
B. Access Control Lists (ACLs).
C. Bucket Policies.
D. All of the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The AWS IT infrastructure that AWS provides, complies with the following IT security standards, including:

A. SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2 and SOC 3
B. FISMA, DIACAP, and FedRAMP
C. PCI DSS Level 1, ISO 27001, ITAR and FIPS 140-2
D. HIPAA, Cloud Security Alliance (CSA) and Motion Picture Association of America (MPAA)E. All of the above

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Auto Scaling requests are signed with a _________ signature calculated from the request and the user’s private key.

A. SSL
B. AES-256
C. HMAC-SHA1
D. X.509

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 19
The following policy can be attached to an IAM group. It lets an IAM user in that group access a "home directory" in AWS S3 that matches their user name using the console.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Action": ["s3:*"],
"Effect": "Allow",
"Resource": ["arn:aws:s3:::bucket-name"],
"Condition":{"StringLike":{"s3:prefix":["home/${aws:username}/*"]}}
},
{
"Action":["s3:*"],
"Effect":"Allow",
"Resource": ["arn:aws:s3:::bucket-name/home/${aws:username}/*"]
}
]
}
```

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 What does elasticity mean to AWS?

A. The ability to scale computing resources up easily, with minimal friction and down with latency.
B. The ability to scale computing resources up and down easily, with minimal friction.
C. The ability to provision cloud computing resources in expectation of future demand.
D. The ability to recover from business continuity events with minimal friction.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 The following are AWS Storage services?
Choose 2 Answers

A. AWS Relational Database Service (AWS RDS)
B. AWS ElastiCache
C. AWS Glacier
D. AWS Import/Export

Correct Answer: BD

Section: (none)
Explanation
Explanation/Reference:

QUESTION 22 How is AWS readily distinguished from other vendors in the traditional IT computing landscape?

A. Experienced. Scalable and elastic. Secure. Cost-effective. Reliable
B. Secure. Flexible. Cost-effective. Scalable and elastic. GlobalC. Secure. Flexible. Cost-effective. Scalable and elastic. Experienced
D. Flexible. Cost-effective. Dynamic. Secure. Experienced.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
You have launched an EC2 instance with four (4) 500 GB EBS Provisioned IOPS volumes attached. The EC2 instance is EBS-Optimized and supports 500 Mbps throughput between EC2 and EBS. The four EBS volumes are configured as a single RAID 0 device, and each Provisioned IOPS volume is provisioned with 4,000 IOPS (4,000 16KB reads or writes), for a total of 16,000 random IOPS on the instance. The EC2 instance initially delivers the expected 16,000 IOPS random read and write performance. Sometime later, in order to increase the total random I/O performance of the instance, you add an additional two 500 GB EBS Provisioned IOPS volumes to the RAID. Each volume is provisioned to 4,000 IOPs like the original four, for a total of 24,000 IOPS on the EC2 instance. Monitoring shows that the EC2 instance CPU utilization increased from 50% to 70%, but the total random IOPS measured at the instance level does not increase at all.

What is the problem and a valid solution?

A. The EBS-Optimized throughput limits the total IOPS that can be utilized; use an EBSOptimized instance that provides larger throughput.
B. Small block sizes cause performance degradation, limiting the I/O throughput; configure the instance device driver and filesystem to use 64KB blocks to increase throughput.
C. The standard EBS Instance root volume limits the total IOPS rate; change the instance root volume to also be a 500GB 4,000 Provisioned IOPS volume.
D. Larger storage volumes support higher Provisioned IOPS rates; increase the provisioned volume storage of each of the 6 EBS volumes to 1TB.
E. RAID 0 only scales linearly to about 4 devices; use RAID 0 with 4 EBS Provisioned IOPS volumes, but increase each Provisioned IOPS EBS volume to 6,000 IOPS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Your company is storing millions of sensitive transactions across thousands of 100-GB files that must be encrypted in transit and at rest. Analysts concurrently depend on subsets of files, which can consume up to 5 TB of space, to generate simulations that can be used to steer business decisions.

You are required to design an AWS solution that can cost effectively accommodate the long-term storage and in-flight subsets of data.

Which approach can satisfy these objectives?

A. Use Amazon Simple Storage Service (S3) with server-side encryption, and run simulations on subsets in ephemeral drives on Amazon EC2.
B. Use Amazon S3 with server-side encryption, and run simulations on subsets in-memory on Amazon EC2.
C. Use HDFS on Amazon EMR, and run simulations on subsets in ephemeral drives on Amazon EC2.
D. Use HDFS on Amazon Elastic MapReduce (EMR), and run simulations on subsets in-memory on Amazon Elastic Compute Cloud (EC2).
E. Store the full data set in encrypted Amazon Elastic Block Store (EBS) volumes, and regularly capture snapshots that can be cloned to EC2 workstations.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 25
Your customer is willing to consolidate their log streams (access logs, application logs, security logs, etc.) in one single system. Once consolidated, the customer wants to analyze these logs in real time based on heuristics. From time to time, the customer needs to validate heuristics, which requires going back to data samples extracted from the last 12 hours.

What is the best approach to meet your customer's requirements?

A. Send all the log events to Amazon SQS, setup an Auto Scaling group of EC2 servers to consume the logs and apply the heuristics.
B. Send all the log events to Amazon Kinesis, develop a client process to apply heuristics on the logs
C. Configure Amazon CloudTrail to receive custom logs, use EMR to apply heuristics the logs
D. Setup an Auto Scaling group of EC2 syslogd servers, store the logs on S3, use EMR to apply heuristics on the logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The throughput of an Amazon Kinesis stream is designed to scale without limits via increasing the number of shards within a stream. However, there are certain limits you should keep in mind while using Amazon Kinesis Streams:
By default, Records of a stream are accessible for up to 24 hours from the time they are added to the stream. You can raise this limit to up to 7 days by enabling extended data retention. The maximum size of a data blob (the data payload before Base64-encoding) within one record is 1 megabyte (MB).
Each shard can support up to 1000 PUT records per second.
For more information about other API level limits, see Amazon Kinesis Streams Limits.

QUESTION 26
A newspaper organization has an on-premises application which allows the public to search its back catalogue and retrieve individual newspaper pages via a website written in Java. They have scanned the old newspapers into JPEGs (approx 17TB) and used Optical Character Recognition (OCR) to populate a commercial search product. The hosting platform and software are now end of life and the organization wants to migrate Its archive to AWS and produce a cost efficient architecture and still be designed for availability and durability.

Which is the most appropriate?

A. Use S3 with reduced redundancy lo store and serve the scanned files, install the commercial search application on EC2 Instances and configure with auto-scaling and an Elastic Load Balancer.
B. Model the environment using CloudFormation use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index.
C. Use S3 with standard redundancy to store and serve the scanned files, use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.
D. Use a single-AZ RDS MySQL instance lo store the search index 33d the JPEG images use an EC2 instance to serve the website and translate user queries into SQL.
E. Use a CloudFront download distribution to serve the JPEGs to the end users and Install the current commercial search product, along with a Java Container Tor the website on EC2 instances and use Route53 with DNS round-robin.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There is no such thing as "Most appropriate" without knowing all your goals. I find your scenarios very fuzzy, since you can obviously mix-n-match between them. I think you should decide by layers instead:
Load Balancer Layer: ELB or just DNS, or roll-your-own. (Using DNS+EIPs is slightly cheaper, but less reliable than ELB.)
Storage Layer for 17TB of Images: This is the perfect use case for S3. Off-load all the web requests directly to the relevant JPEGs in S3. Your EC2 boxes just generate links to them.
If your app already serves it's own images (not links to images), you might start with EFS. But more than likely, you can just setup a web server to re-write or re-direct all JPEG links to S3 pretty easily. If you use S3, don't serve directly from the bucket - Serve via a CNAME in domain you control. That way, you can switch in CloudFront easily.
EBS will be way more expensive, and you'll need 2x the drives if you need 2 boxes. Yuck.
Consider a smaller storage format. For example, JPEG200 or WebP or other tools might make for smaller images. There is also the DejaVu format from a while back.
Cache Layer: Adding CloudFront in front of S3 will help people on the other side of the world -- well, possibly. Typical archives follow a power law. The long tail of requests means that most JPEGs won't be requested enough to be in the cache. So you are only speeding up the most popular objects. You can always wait, and switch in CF later after you know your costs better. (In some cases, it can actually lower costs.)
You can also put CloudFront in front of your app, since your archive search results should be fairly static. This will also allow you to run with a smaller instance type, since CF will handle much of the load if you do it right.
Database Layer: A few options:
Use whatever your current server does for now, and replace with something else down the road. Don't under-estimate this approach, sometimes it's better to start now and optimize later. Use RDS to run MySQL/Postgres
I'm not as familiar with ElasticSearch / Cloudsearch, but obviously Cloudsearch will be less maintenance+setup. App Layer:

When creating the app layer from scratch, consider CloudFormation and/or OpsWorks. It's extra stuff to learn, but helps down the road. Java+Tomcat is right up the alley of ElasticBeanstalk. (Basically EC2 + Autoscale + ELB).
Preventing Abuse: When you put something in a public S3 bucket, people will hot-link it from their web pages. If you want to prevent that, your app on the EC2 box can generate signed links to S3 that expire in a few hours. Now everyone will be forced to go thru the app, and the app can apply rate limiting, etc.
Saving money: If you don't mind having downtime:
run everything in one AZ (both DBs and EC2s). You can always add servers and AZs down the road, as long as it's architected to be stateless. In fact, you should use multiple regions if you want it to be really robust. use Reduced Redundancy in S3 to save a few hundred bucks per month (Someone will have to "go fix it" every time it breaks, including having an off-line copy to repair S3.)
Buy Reserved Instances on your EC2 boxes to make them cheaper. (Start with the RI market and buy a partially used one to get started.) It's just a coupon saying "if you run this type of box in this AZ, you will save on the per-hour costs." You can get 1/2 to 1/3 off easily.
Rewrite the application to use less memory and CPU - that way you can run on fewer/smaller boxes. (May or may not be worth the investment.)
If your app will be used very infrequently, you will save a lot of money by using Lambda. I'd be worried that it would be quite slow if you tried to run a Java application on it though.
We're missing some information like load, latency expectations from search, indexing speed, size of the search index, etc. But with what you've given us, I would go with S3 as the storage for the files (S3 rocks. It is really, really awesome).
If you're stuck with the commercial search application, then on EC2 instances with autoscaling and an ELB. If you are allowed an alternative search engine, Elasticsearch is probably your best bet. I'd run it on EC2 instead of the AWS Elasticsearch service, as IMHO it's not ready yet. Don't autoscale Elasticsearch automatically though, it'll cause all sorts of issues. I have zero experience with CloudSearch so ic an't comment on that. Regardless of which option, I'd use CloudFormation for all of it.

QUESTION 27

Your company has recently extended its datacenter into a VPC on AVVS to add burst computing capacity as needed Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary You don't want to create new IAM users for each NOC member and make those users sign in again to the AWS Management Console.

Which option below will meet the needs for your NOC members?

A. Use OAuth 2 0 to retrieve temporary AWS security credentials to enable your NOC members to sign in to the AWS Management Console.
B. Use web Identity Federation to retrieve AWS temporary security credentials to enable your NOC members to sign in to the AWS Management Console.
C. Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the NOC members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.
D. Use your on-premises SAML 2.0-compliam identity provider (IDP) to retrieve temporary security credentials to enable NOC members to sign in to the AWS Management Console.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

QUESTION 28

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

Identify which option will allow you to achieve this goal.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bucket Owner Granting Cross-account Permission to objects It Does Not Own
In this example scenario, you own a bucket and you have enabled other AWS accounts to upload objects. That is, your bucket can have objects that other AWS accounts own.
Now, suppose as a bucket owner, you need to grant cross-account permission on objects, regardless of who the owner is, to a user in another account. For example, that user could be a billing application that needs to access object metadata. There are two core issues:
The bucket owner has no permissions on those objects created by other AWS accounts. So for the bucket owner to grant permissions on objects it does not own, the object owner, the AWS account that created the objects, must first grant permission to the bucket owner. The bucket owner can then delegate those permissions.
Bucket owner account can delegate permissions to users in its own account but it cannot delegate permissions to other AWS accounts, because cross-account delegation is not supported.

In this scenario, the bucket owner can create an AWS Identity and Access Management (IAM) role with permission to access objects, and grant another AWS account permission to assume the role temporarily enabling it to access objects in the bucket.

Background: Cross-Account Permissions and Using IAM Roles

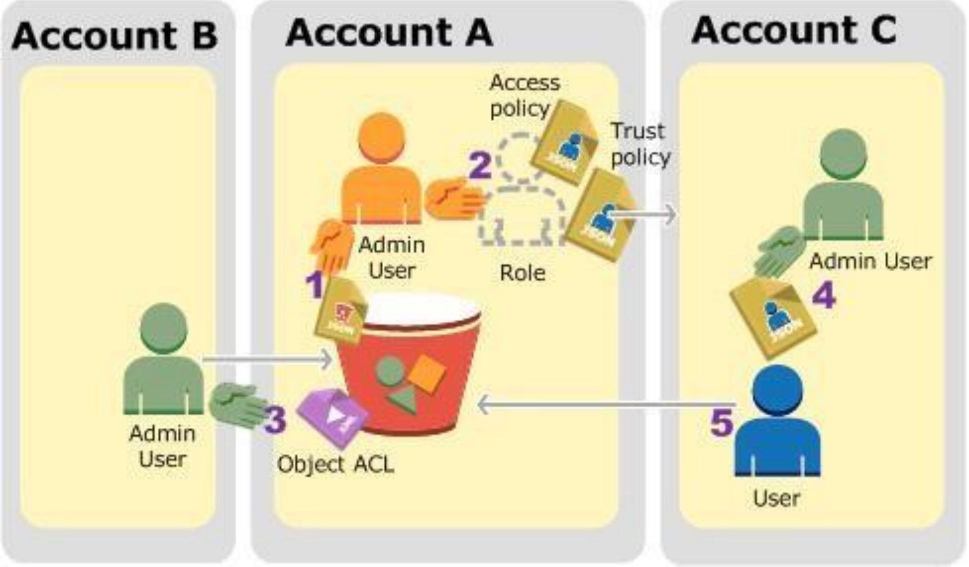
IAM roles enable several scenarios to delegate access to your resources, and cross-account access is one of the key scenarios. In this example, the bucket owner, Account A, uses an IAM role to temporarily delegate object access crossaccount to users in another AWS account, Account C. Each IAM role you create has two policies attached to it: A trust policy identifying another AWS account that can assume the role.

An access policy defining what permissions—for example, s3:GetObject—are allowed when someone assumes the role. For a list of permissions you can specify in a policy, see Specifying Permissions in a Policy.

The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects: Assume the role and, in response, get temporary security credentials.

Using the temporary security credentials, access the objects in the bucket.

For more information about IAM roles, go to Roles (Delegation and Federation) in IAM User Guide. The following is a summary of the walkthrough steps:



Account A administrator user attaches a bucket policy granting Account B conditional permission to upload objects.

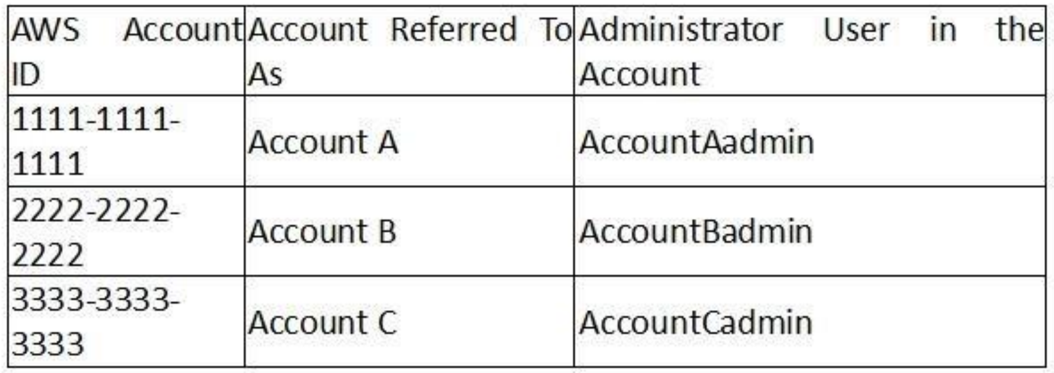
Account A administrator creates an IAM role, establishing trust with Account C, so users in that account can access Account A. The access policy attached to the role limits what user in Account C can do when the user accesses Account A.

Account B administrator uploads an object to the bucket owned by Account A, granting full-control permission to the bucket owner.

Account C administrator creates a user and attaches a user policy that allows the user to assume the role.

User in Account C first assumes the role, which returns the user temporary security credentials. Using those temporary credentials, the user then accesses objects in the bucket.

For this example, you need three accounts. The following table shows how we refer to these accounts and the administrator users in these accounts. Per IAM guidelines (see About Using an Administrator User to Create Resources and Grant Permissions) we do not use the account root credentials in this walkthrough. Instead, you create an administrator user in each account and use those credentials in creating resources and granting them permissions



AWS Account ID	Account Referred To As	Administrator User in the Account
1111-1111-1111	Account A	AccountAadmin
2222-2222-2222	Account B	AccountBadmin
3333-3333-3333	Account C	AccountCadmin

QUESTION 29

You're running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible block-based storage. You have 140TB of data and would like to mount it as a single folder on your file server. Users must be able to access portions of this data while the backups are taking place.

What backup solution would be most appropriate for this use case?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Volume gateway provides an iSCSI target, which enables you to create volumes and mount them as iSCSI devices from your on-premises application servers. The volume gateway runs in either a cached or stored mode.

In the cached mode, your primary data is written to S3, while you retain some portion of it locally in a cache for frequently accessed data.
In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.
In either mode, you can take point-in-time snapshots of your volumes and store them in Amazon S3, enabling you to make space-efficient versioned copies of your volumes for data protection and various data reuse needs.

QUESTION 30
To serve Web traffic for a popular product your chief financial officer and IT director have purchased 10 m1.large heavy utilization Reserved Instances (RIs), evenly spread across two availability zones; Route 53 is used to deliver the traffic to an Elastic Load Balancer (ELB). After several months, the product grows even more popular and you need additional capacity. As a result, your company purchases two C3.2xlarge medium utilization Ris. You register the two c3.2xlarge instances with your ELB and quickly find that the m1.large instances are at 100% of capacity and the c3.2xlarge instances have significant capacity that's unused.

Which option is the most cost effective and uses EC2 capacity most effectively?

A. Configure Autoscaling group and Launch Configuration with ELB to add up to 10 more on-demand m1.large instances when triggered by Cloudwatch. Shut off c3.2xlarge instances.
B. Configure ELB with two c3.2xlarge instances and use on-demand Autoscaling group for up to two additional c3.2xlarge instances. Shut off m1.large instances.
C. Route traffic to EC2 m1.large and c3.2xlarge instances directly using Route 53 latency based routing and health checks. Shut off ELB.
D. Use a separate ELB for each instance type and distribute load to ELBs with Route 53 weighted round robin.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

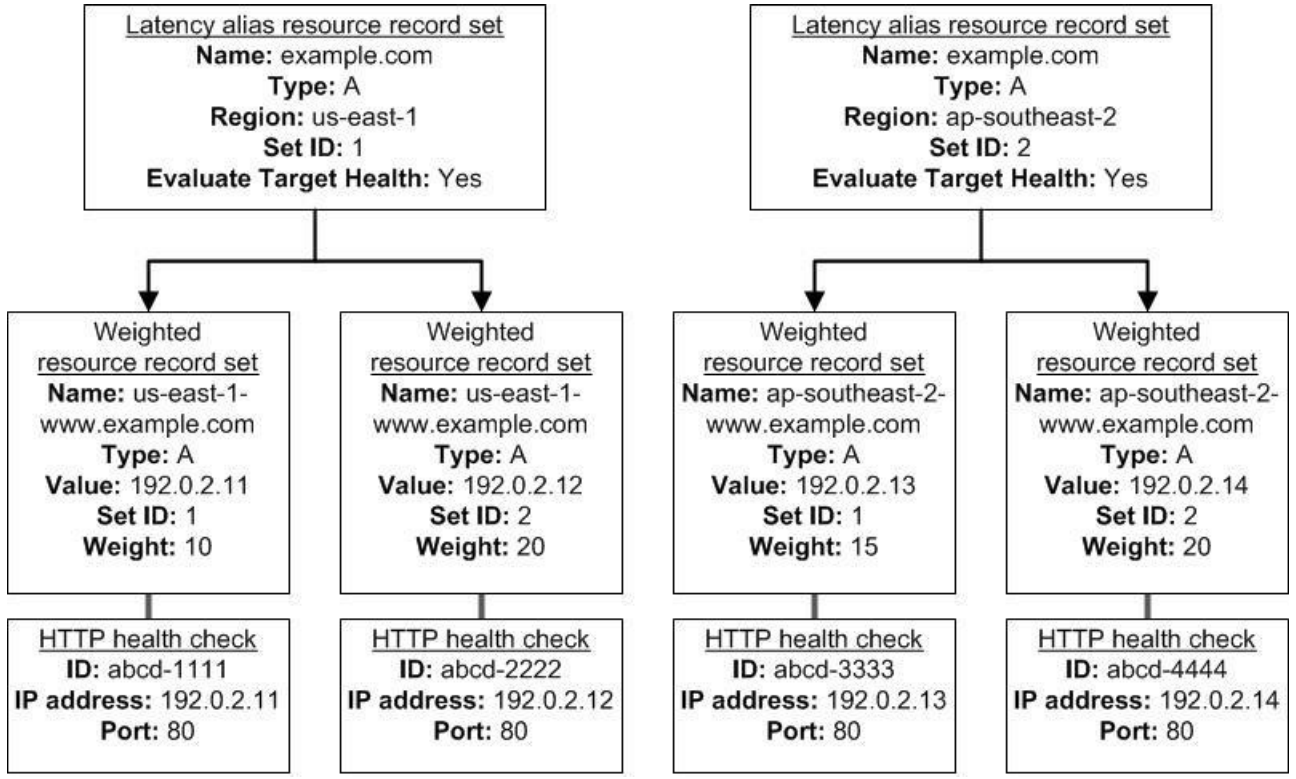
QUESTION 31
You have deployed a web application targeting a global audience across multiple AWS Regions under the domain name.example.com. You decide to use Route53 Latency-Based Routing to serve web requests to users from the region closest to the user. To provide business continuity in the event of server downtime you configure weighted record sets associated with two web servers in separate Availability Zones per region. Dunning a DR test you notice that when you disable all web servers in one of the regions Route53 does not automatically direct all users to the other region.

What could be happening? (Choose 2 answers)

A. Latency resource record sets cannot be used in combination with weighted resource record sets.
B. You did not setup an HTTP health check to one or more of the weighted resource record sets associated with me disabled web servers.
C. The value of the weight associated with the latency alias resource record set in the region with the disabled servers is higher than the weight for the other region.
D. One of the two working web servers in the other region did not pass its HTTP health check.
E. You did not set "Evaluate Target Health" to "Yes" on the latency alias resource record set associated with example com in the region where you disabled the servers.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
How Health Checks Work in Complex Amazon Route 53 Configurations
Checking the health of resources in complex configurations works much the same way as in simple configurations. However, in complex configurations, you use a combination of alias resource record sets (including weighted alias, latency alias, and failover alias) and nonalias resource record sets to build a decision tree that gives you greater control over how Amazon Route 53 responds to requests. For more information, see How Health Checks Work in Simple Amazon Route 53 Configurations.
For example, you might use latency alias resource record sets to select a region close to a user and use weighted resource record sets for two or more resources within each region to protect against the failure of a single endpoint or an Availability Zone. The following diagram shows this configuration.



Here's how Amazon EC2 and Amazon Route 53 are configured:

You have Amazon EC2 instances in two regions, us-east-1 and ap-southeast-2. You want Amazon Route 53 to respond to queries by using the resource record sets in the region that provides the lowest latency for your customers, so you create a latency alias resource record set for each region. (You create the latency alias resource record sets after you create resource record sets for the individual Amazon EC2 instances.)

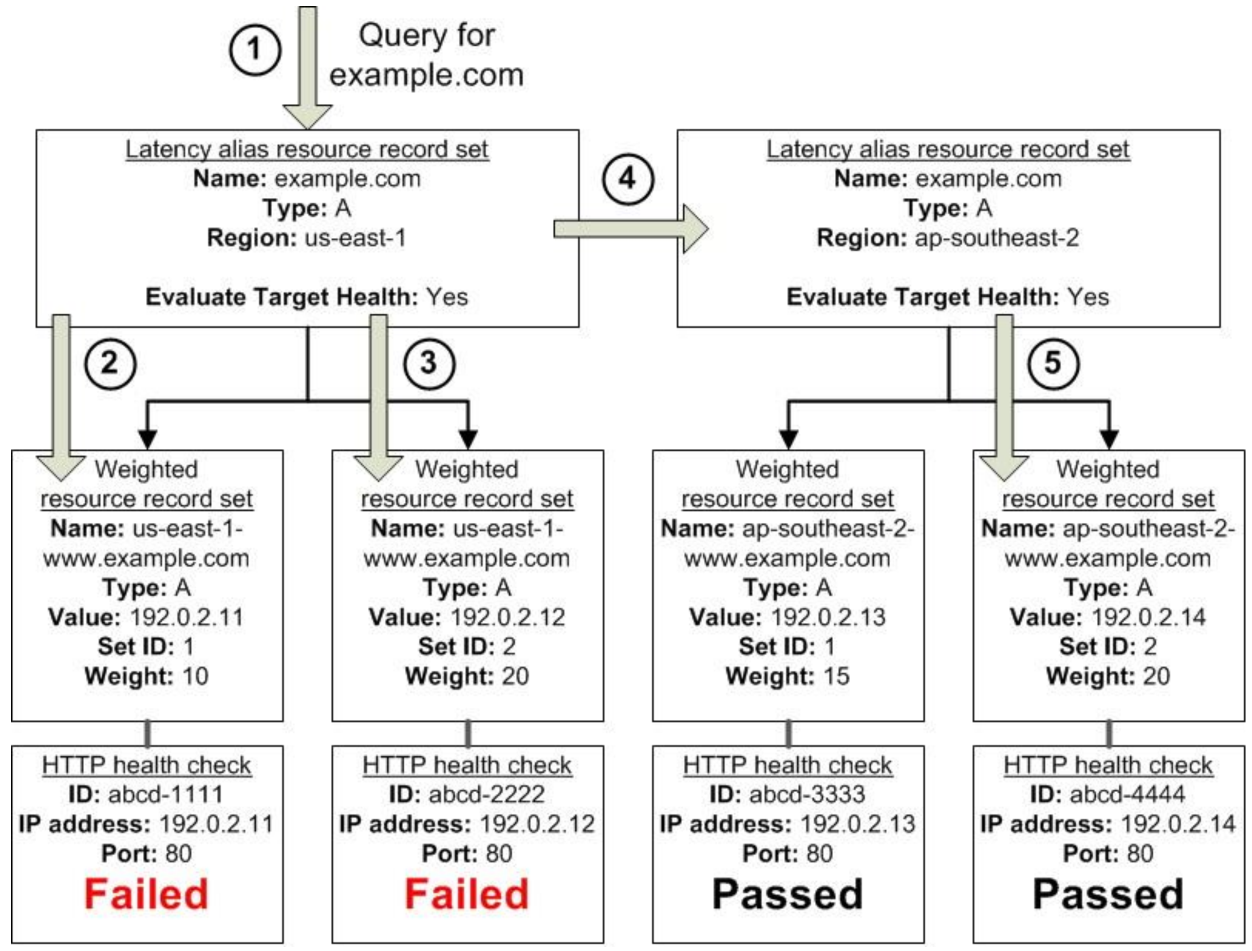
Within each region, you have two Amazon EC2 instances. You create a weighted resource record set for each instance. The name and the type are the same for both of the weighted resource record sets in each region.

When you have multiple resources in a region, you can create weighted or failover resource record sets for your resources. You can also create even more complex configurations by creating weighted alias or failover alias resource record sets that, in turn, refer to multiple resources.

Each weighted resource record set has an associated health check. The IP address for each health check matches the IP address for the corresponding resource record set. This isn't required, but it's the most common configuration.

For both latency alias resource record sets, you set the value of Evaluate Target Health to Yes.

You use the Evaluate Target Health setting for each latency alias resource record set to make Amazon Route 53 evaluate the health of the alias targets—the weighted resource record sets—and respond accordingly.



The preceding diagram illustrates the following sequence of events:

Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.

Amazon Route 53 selects a weighted resource record set based on weight. Evaluate Target Health is Yes for the latency alias resource record set, so Amazon Route 53 checks the health of the selected weighted resource record set.

The health check failed, so Amazon Route 53 chooses another weighted resource record set based on weight and checks its health. That resource record set also is unhealthy.

Amazon Route 53 backs out of that branch of the tree, looks for the latency alias resource record set with the next-best latency, and chooses the resource record set for ap-southeast-2.

Amazon Route 53 again selects a resource record set based on weight, and then checks the health of the selected resource record set. The health check passed, so Amazon Route 53 returns the applicable value in response to the query.

What Happens When You Associate a Health Check with an Alias Resource Record Set?

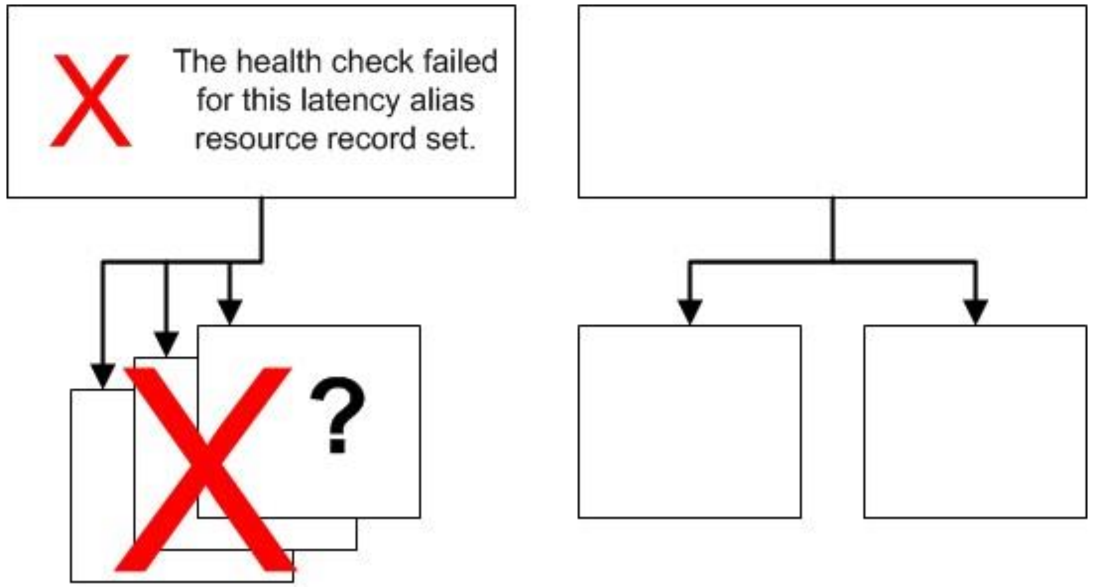
You can associate a health check with an alias resource record set instead of or in addition to setting the value of Evaluate Target Health to Yes. However, it's generally more useful if Amazon Route 53 responds to queries based on the health of the underlying resources—the HTTP servers, database servers, and other resources that your alias resource record sets refer to. For example, suppose the following configuration:

You assign a health check to a latency alias resource record set for which the alias target is a group of weighted resource record sets.

You set the value of Evaluate Target Health to Yes for the latency alias resource record set.

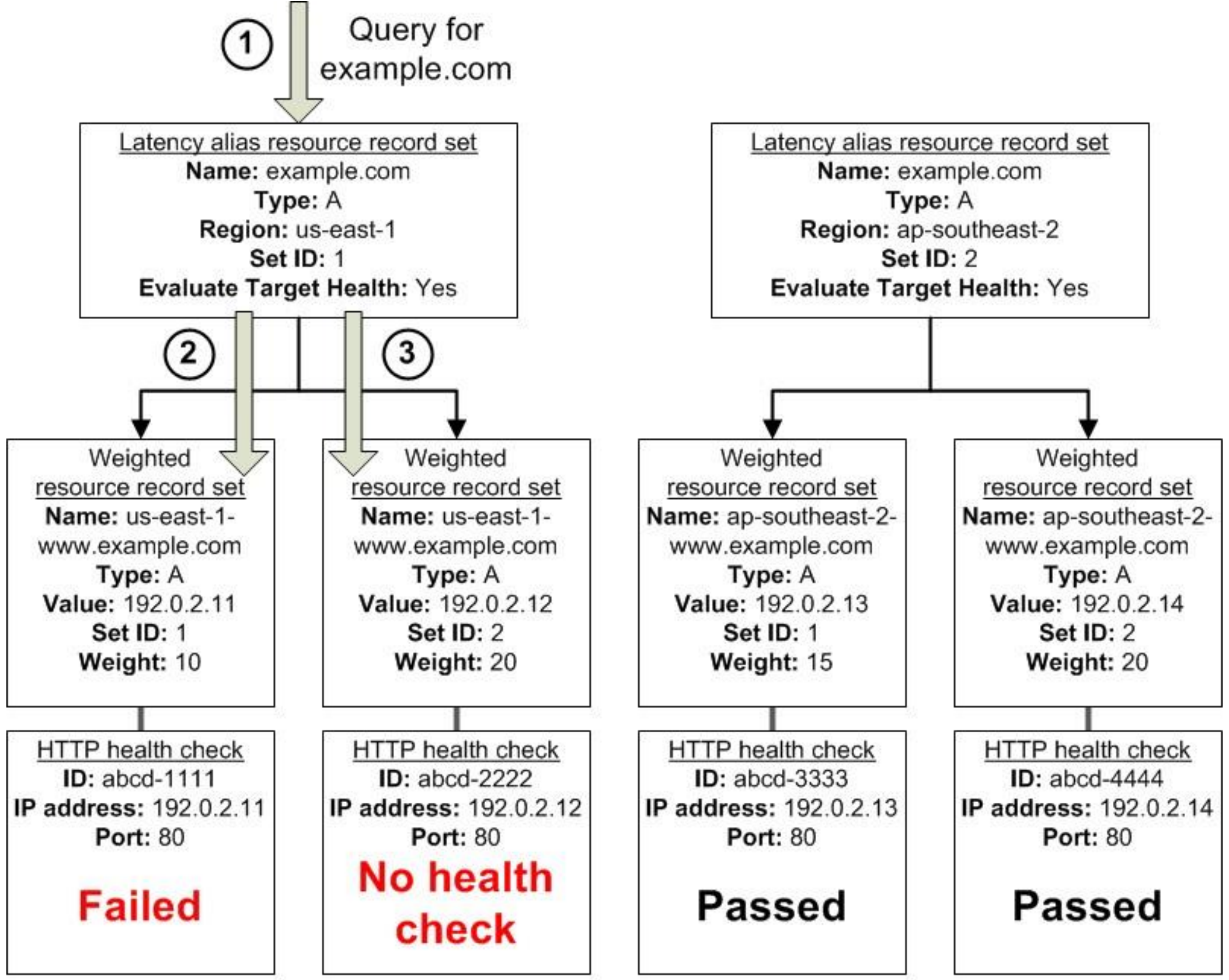
In this configuration, both of the following must be true before Amazon Route 53 will return the applicable value for a weighted resource record set: The health check associated with the latency alias resource record set must pass.

At least one weighted resource record set must be considered healthy, either because it's associated with a health check that passes or because it's not associated with a health check. In the latter case, Amazon Route 53 always considers the weighted resource record set healthy.


The health check failed for this latency alias resource record set.
?

If the health check for the latency alias resource record set fails, Amazon Route 53 stops responding to queries using any of the weighted resource record sets in the alias target, even if they're all healthy. Amazon Route 53 doesn't know the status of the weighted resource record sets because it never looks past the failed health check on the alias resource record set. What Happens When You Omit Health Checks?

In a complex configuration, it's important to associate health checks with all of the non-alias resource record sets. Let's return to the preceding example, but assume that a health check is missing on one of the weighted resource record sets in the us-east-1 region:



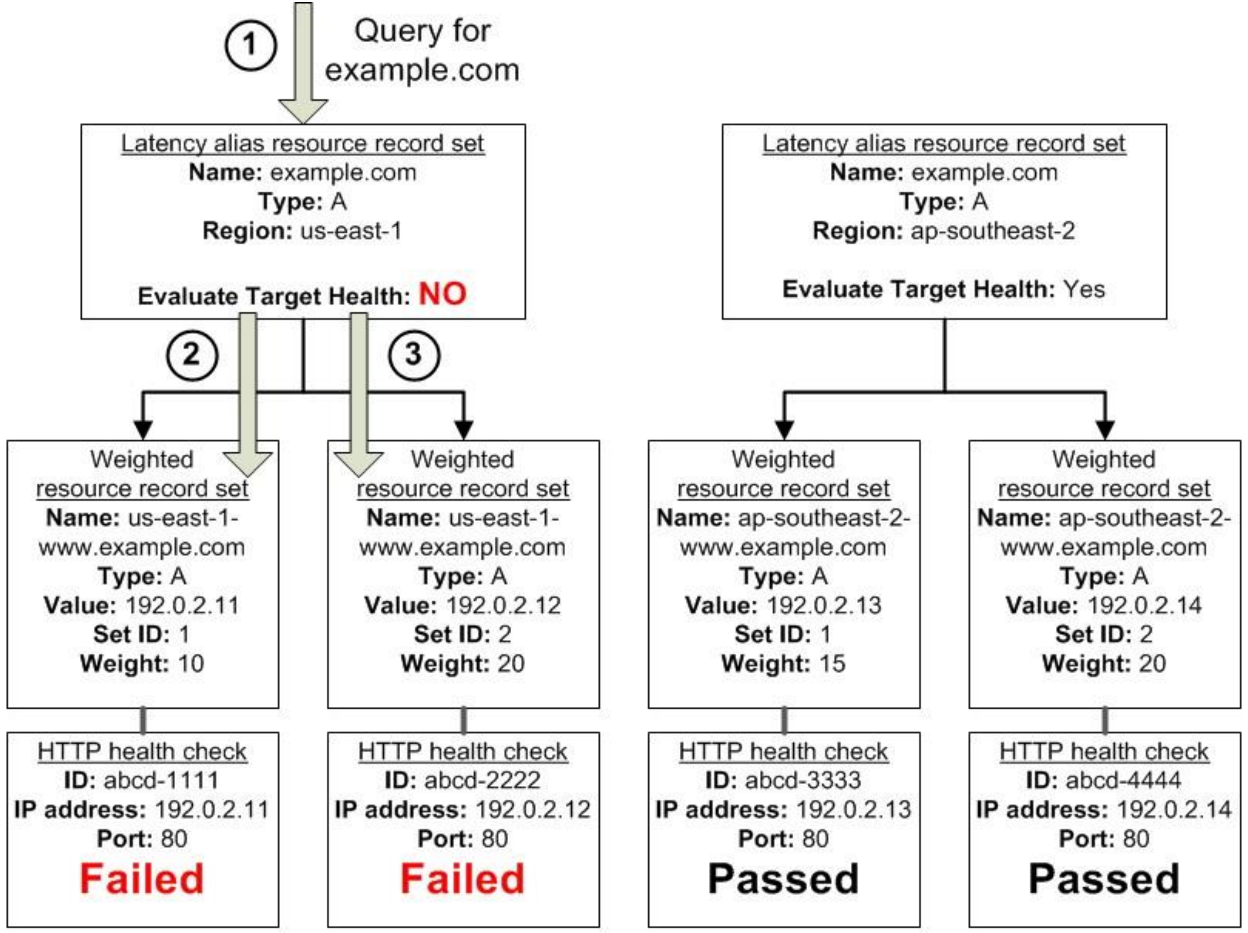
Here's what happens when you omit a health check on a non-alias resource record set in this configuration:

Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.

Amazon Route 53 looks up the alias target for the latency alias resource record set, and checks the status of the corresponding health checks. The health check for one weighted resource record set failed, so that resource record set is omitted from consideration.

The other weighted resource record set in the alias target for the us-east-1 region has no health check. The corresponding resource might or might not be healthy, but without a health check, Amazon Route 53 has no way to know. Amazon Route 53 assumes that the resource is healthy and returns the applicable value in response to the query. What Happens When You Set Evaluate Target Health to No?

In general, you also want to set Evaluate Target Health to Yes for all of the alias resource record sets. In the following example, all of the weighted resource record sets have associated health checks, but Evaluate Target Health is set to No for the latency alias resource record set for the us-east-1 region:



Here's what happens when you set Evaluate Target Health to No for an alias resource record set in this configuration:

Amazon Route 53 receives a query for example.com. Based on the latency for the user making the request, Amazon Route 53 selects the latency alias resource record set for the us-east-1 region.

Amazon Route 53 determines what the alias target is for the latency alias resource record set, and checks the corresponding health checks. They're both failing.

Because the value of Evaluate Target Health is No for the latency alias resource record set for the us-east-1 region, Amazon Route 53 must choose one resource record set in this branch instead of backing out of the branch and looking for a healthy resource record set in the ap-southeast-2 region.

QUESTION 32

Your startup wants to implement an order fulfillment process for selling a personalized gadget that needs an average of 3-4 days to produce with some orders taking up to 6 months you expect 10 orders per day on your first day. 1000 orders per day after 6 months and 10,000 orders after 12 months.

Orders coming in are checked for consistency men dispatched to your manufacturing plant for production quality control packaging shipment and payment processing If the product does not meet the quality standards at any stage of the process employees may force the process to repeat a step Customers are notified via email about order status and any critical issues with their orders such as payment failure.

Your base architecture includes AWS Elastic Beanstalk for your website with an RDS MySQL instance for customer data and orders.

How can you implement the order fulfillment process while making sure that the emails are delivered reliably?

A. Add a business process management application to your Elastic Beanstalk app servers and re-use the ROS database for tracking order status use one of the Elastic Beanstalk instances to send emails to customers.

B. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1 Use the decider instance to send emails to customers.

C. Use SWF with an Auto Scaling group of activity workers and a decider instance in another Auto Scaling group with min/max=1 use SES to send emails to customers.

D. Use an SQS queue to manage all process tasks Use an Auto Scaling group of EC2 Instances that poll the tasks and execute them. Use SES to send emails to customers.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 33 A read only news reporting site with a combined web and application tier and a database tier that receives large and unpredictable traffic demands must be able to respond to these traffic fluctuations automatically.

What AWS services should be used meet these requirements?

A. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaimg group monitored with CloudWatch and RDS with read replicas.
B. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and RDS with read replicas.
C. Stateful instances for the web and application tier in an autoscaling group monitored with CloudWatch and multi-AZ RDS.
D. Stateless instances for the web and application tier synchronized using ElastiCache Memcached in an autoscaling group monitored with CloudWatch and multi-AZ RDS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
You are designing a photo-sharing mobile app. The application will store all pictures in a single Amazon S3 bucket.
Users will upload pictures from their mobile device directly to Amazon S3 and will be able to view and download their own pictures directly from Amazon S3. You want to configure security to handle potentially millions of users in the most secure manner possible.

What should your server-side application do when a new user registers on the photo-sharing mobile application?

A. Create an IAM user. Update the bucket policy with appropriate permissions for the IAM user. Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
B. Create an IAM user. Assign appropriate permissions to the IAM user. Generate an access key and secret key for the IAM user, store them in the mobile app and use these credentials to access Amazon S3.
C. Create a set of long-term credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app and use them to access Amazon S3.
D. Record the user's information in Amazon RDS and create a role in IAM with appropriate permissions. When the user uses their mobile app, create temporary credentials using the AWS Security Token Service "AssumeRole" function.Store these credentials in the mobile app's memory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.
E. Record the user's information in Amazon DynamoDB. When the user uses their mobile app, create temporary credentials using AWS Security Token Service with appropriate permissions. Store these credentials in the mobile app'smemory and use them to access Amazon S3. Generate new credentials the next time the user runs the mobile app.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
You are tasked with moving a legacy application from a virtual machine running inside your datacenter to an Amazon VPC. Unfortunately, this app requires access to a number of on-premises services and no one who configured the app still works for your company. Even worse there's no documentation for it.

What will allow the application running inside the VPC to reach back and access its internal dependencies without being reconfigured? (Choose 3 answers)

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

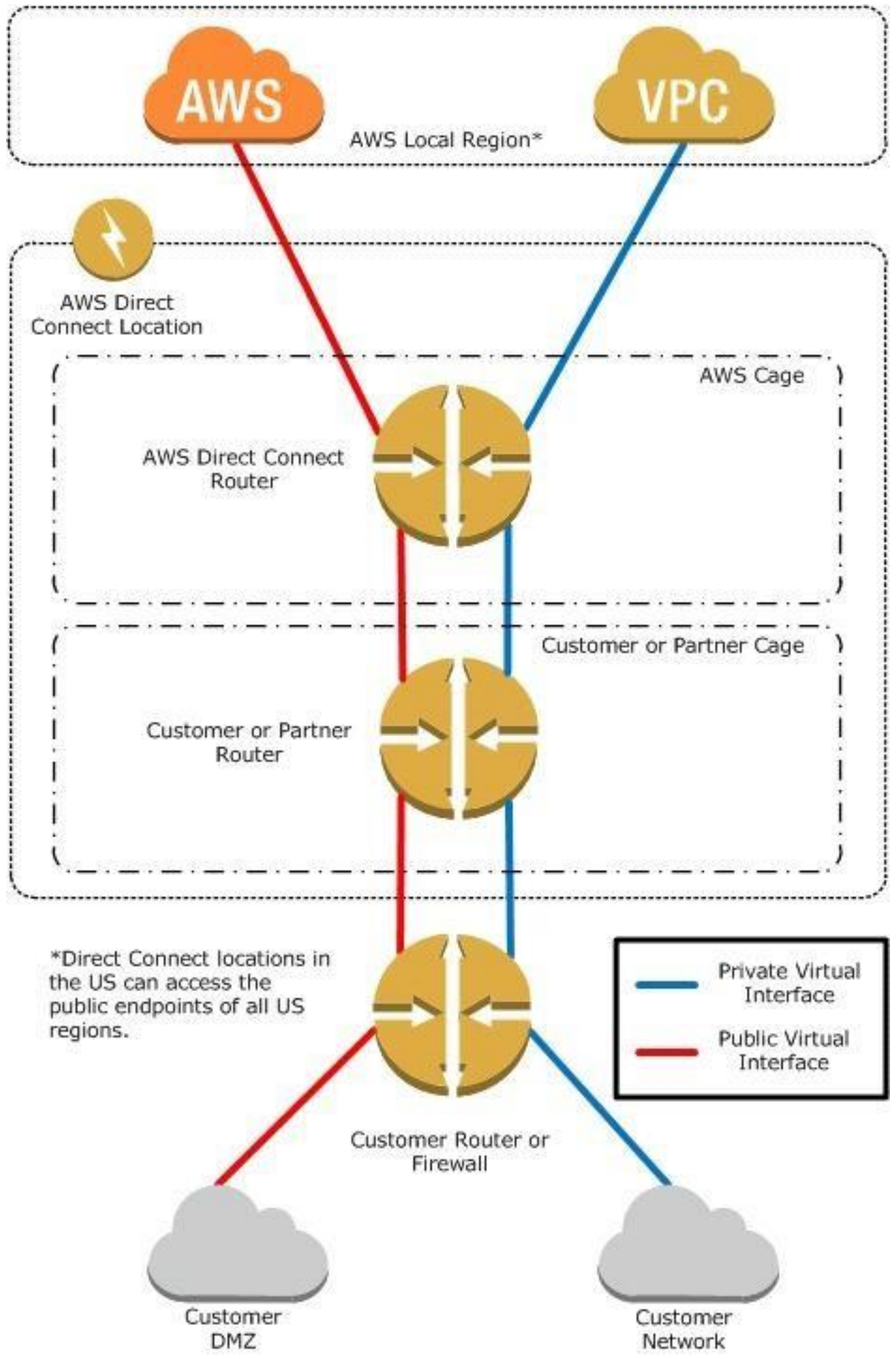
Correct Answer: ADF
Section: (none)
Explanation
Explanation/Reference:
Explanation:
AWS Direct Connect

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

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space, while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.

What is AWS Direct Connect?

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to the AWS cloud (for example, to Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3) and to Amazon Virtual Private Cloud (Amazon VPC), bypassing Internet service providers in your network path. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. For example, you can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US). The following diagram shows how AWS Direct Connect interfaces with your network.


AWS
VPC
AWS Local Region*
AWS Direct Connect Location
AWS Cage
AWS Direct Connect Router
Customer or Partner Cage
Customer or Partner Router
*Direct Connect locations in the US can access the public endpoints of all US regions.
Private Virtual Interface
Public Virtual Interface
Customer Router or Firewall
Customer DMZ
Customer Network

Requirements

To use AWS Direct Connect, your network must meet one of the following conditions:

Your network is collocated with an existing AWS Direct Connect location. For more information on available AWS Direct Connect locations, go to http://aws.amazon.com/directconnect/.

You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN). For a list of AWS Direct Connect partners who can help you connect, go to http://aws.amazon.com/directconnect. You are working with an independent service provider to connect to AWS Direct Connect.

In addition, your network must meet the following conditions:

Connections to AWS Direct Connect require single mode fiber, 1000BASE-LX (1310nm) for 1 gigabit Ethernet, or 10GBASE-LR (1310nm) for 10 gigabit Ethernet. Auto Negotiation for the port must be disabled. You must support 802.1Q VLANs across these connections.

Your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication. Optionally, you may configure Bidirectional Forwarding Detection (BFD).

To connect to Amazon Virtual Private Cloud (Amazon VPC), you must first do the following:

Provide a private Autonomous System Number (ASN). Amazon allocates a private IP address in the 169.x.x.x range to you.

Create a virtual private gateway and attach it to your VPC. For more information about creating a virtual private gateway, see Adding a Hardware Virtual Private Gateway to Your VPC in the Amazon VPC User Guide.

To connect to public AWS products such as Amazon EC2 and Amazon S3, you need to provide the following: A public ASN that you own (preferred) or a private ASN.

Public IP addresses (/31) (that is, one for each end of the BGP session) for each BGP session. If you do not have public IP addresses to assign to this connection, log on to AWS and then open a ticket with AWS Support. The public routes that you will advertise over BGP.

QUESTION 36

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use a block device. Amazon EBS volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component.
Amazon EBS provides three volume types: General Purpose (SSD), Provisioned IOPS (SSD), and Magnetic. The three volume types differ in performance characteristics and cost, so you can choose the right storage performance and price for the needs of your applications. All EBS volume types offer the same durable snapshot capabilities and are designed for 99.999% availability.

QUESTION 37

You have been asked to design the storage layer for an application. The application requires disk performance of at least 100,000 IOPS. In addition, the storage layer must be able to survive the loss of an individual disk, EC2 instance, or Availability Zone without any data loss. The volume you provide must have a capacity of at least 3 TB.

Which of the following designs will meet these objectives?

A. Instantiate a c3.8xlarge instance in us-east-1. Provision 4x1TB EBS volumes, attach them to the instance, and configure them as a single RAID 5 volume. Ensure that EBS snapshots are performed every 15 minutes.
B. Instantiate a c3.8xlarge instance in us-east-1. Provision 3xlTB EBS volumes, attach them to the Instance, and configure them as a single RAID 0 volume. Ensure that EBS snapshots are performed every 15 minutes.
C. Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Provision 3x1TB EBS volumes, attach them to the instance, and configure them as asecond RAID 0 volume. Configure synchronous, block-level replication from the ephemeral-backed volume to the EBS-backed volume.
D. Instantiate a c3.8xlarge instance in us-east-1. Provision an AWS Storage Gateway and configure it for 3 TB of storage and 100,000 IOPS. Attach the volume to the instance.
E. Instantiate an i2.8xlarge instance in us-east-1a. Create a RAID 0 volume using the four 800GB SSD ephemeral disks provided with the instance. Configure synchronous, block-level replication to an identically configured instance in us-east-1b.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation: https://acloud.guru/course/aws-certified-solutions-architect-associate/discuss/-KJdi4tFMp2x_O88J6U4/an-architecture-design-question

QUESTION 38

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

What would you recommend? (Choose 2)

A. Have the mobile app access Amazon DynamoDB directly Instead of JSON files stored on Amazon S3.

B. Write data directly into an Amazon Redshift cluster replacing both Amazon DynamoDB and Amazon S3.
C. Introduce an Amazon SQS queue to buffer writes to the Amazon DynamoDB table and reduce provisioned write throughput.
D. Introduce Amazon Elasticache to cache reads from the Amazon DynamoDB table and reduce provisioned read throughput.
E. Create a new Amazon DynamoDB table each day and drop the one for the previous day after its data is on Amazon S3.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf

QUESTION 39
A large real-estate brokerage is exploring the option of adding a cost-effective location based alert to their existing mobile application. The application backend infrastructure currently runs on AWS. Users who opt in to this service will receive alerts on their mobile device regarding real-estate otters in proximity to their location. For the alerts to be relevant delivery time needs to be in the low minute count the existing mobile app has 5 million users across the US.

Which one of the following architectural suggestions would you make to the customer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
You currently operate a web application. In the AWS US-East region. The application runs on an auto-scaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has tasked you to develop a reliable and durable logging solution to track changes made to your EC2.IAM And RDS resources. The solution must ensure the integrity and confidentiality of your log data.

Which of these solutions would you recommend?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

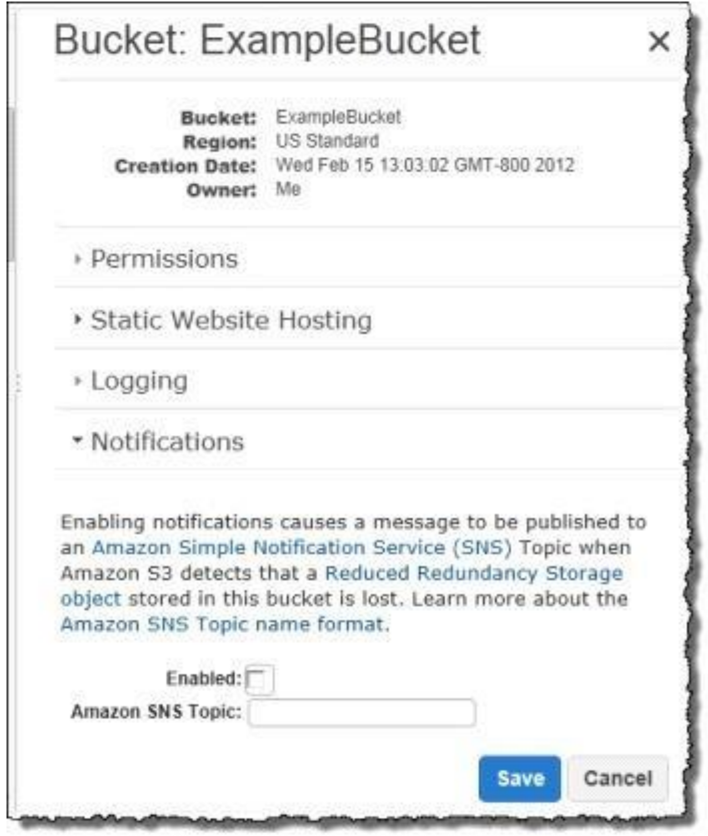
QUESTION 41
Your department creates regular analytics reports from your company's log files All log data is collected in Amazon S3 and processed by daily Amazon Elastic MapReduce (EMR) jobs that generate daily PDF reports and aggregated tables in CSV format for an Amazon Redshift data warehouse.
Your CFO requests that you optimize the cost structure for this system.

Which of the following alternatives will lower costs without compromising average performance of the system or data integrity for the raw data?

A. Use reduced redundancy storage (RRS) for all data In S3. Use a combination of Spot Instances and Reserved Instances for Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
B. Use reduced redundancy storage (RRS) for PDF and .csv data in S3. Add Spot Instances to EMR jobs. Use Spot Instances for Amazon Redshift.
C. Use reduced redundancy storage (RRS) for PDF and .csv data In Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.
D. Use reduced redundancy storage (RRS) for all data in Amazon S3. Add Spot Instances to Amazon EMR jobs. Use Reserved Instances for Amazon Redshift.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using Reduced Redundancy Storage Amazon S3 stores objects according to their storage class. It assigns the storage class to an object when it is written to Amazon S3. You can assign objects a specific storage class (standard or reduced redundancy) only when you write the objects to an Amazon S3 bucket or when you copy objects that are already stored in Amazon S3. Standard is the default storage class. For information about storage classes, see Object Key and Metadata.
In order to reduce storage costs, you can use reduced redundancy storage for noncritical, reproducible data at lower levels of redundancy than Amazon S3 provides with standard storage. The lower level of redundancy results in less durability and availability, but in many cases, the lower costs can make reduced redundancy storage an acceptable storage solution. For example, it can be a cost-effective solution for sharing media content that is durably stored elsewhere. It can also make sense if you are storing thumbnails and other resized images that can be easily reproduced from an original image.
Reduced redundancy storage is designed to provide 99.99% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.01% of objects. For example, if you store 10,000 objects using the RRS option, you can, on average, expect to incur an annual loss of a single object per year (0.01% of 10,000 objects).
Note:
This annual loss represents an expected average and does not guarantee the loss of less than 0.01% of objects in a given year.
Reduced redundancy storage stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but it does not replicate objects as many times as Amazon S3 standard storage. In addition, reduced redundancy storage is designed to sustain the loss of data in a single facility.
If an object in reduced redundancy storage has been lost, Amazon S3 will return a 405 error on requests made to that object. Amazon S3 also offers notifications for reduced redundancy storage object loss: you can configure your bucket so that when Amazon S3 detects the loss of an RRS object, a notification will be sent through Amazon Simple Notification Service (Amazon SNS). You can then replace the lost object. To enable notifications, you can use the Amazon S3 console to set the Notifications property of your bucket.



Bucket: ExampleBucket

Bucket: ExampleBucket
Region: US Standard
Creation Date: Wed Feb 15 13:03:02 GMT-800 2012
Owner: Me

Enabling notifications causes a message to be published to an Amazon Simple Notification Service (SNS) Topic when Amazon S3 detects that a Reduced Redundancy Storage object stored in this bucket is lost. Learn more about the Amazon SNS Topic name format.

Enabled: □
Amazon SNS Topic:

QUESTION 42
You require the ability to analyze a large amount of data, which is stored on Amazon S3 using Amazon Elastic Map Reduce. You are using the cc2 8xlarge instance type, whose CPUs are mostly idle during processing. Which of the below would be the most cost efficient way to reduce the runtime of the job? A. Create more, smaller flies on Amazon S3.

B. Add additional cc2 8xlarge instances by introducing a task group.

C. Use smaller instances that have higher aggregate I/O performance.
D. Create fewer, larger files on Amazon S3.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
An AWS customer is deploying an application mat is composed of an AutoScaling group of EC2 Instances.
The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique x 509 certificate that contains the specific instance-id.
In addition, an x 509 certificates must Designed by the customer's Key management service in order to be trusted for authentication.

Which of the following configurations will support these requirements?

A. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure the Auto Scaling group to launch instances with this role. Have the instances bootstrap get the certificate from Amazon S3upon first boot.
B. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group. Have the launched instances generate a certificate signature request with the instance's assigned instance-id to the key management servicefor signature.
C. Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management service generate a signed certificate and send it directly to the newlylaunched instance.
D. Configure the launched instances to generate a new certificate upon first boot. Have the Key management service poll the Auto Scaling group for associated instances and send new instances a certificate signature (hat contains thespecific instance-id.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Your company runs a customer facing event registration site This site is built with a 3-tier architecture with web and application tier servers and a MySQL database The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database.

When deploying this application in a region with three availability zones (AZs) which architecture provides high availability?

A. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 3 EC2 instances ineach AZ inside an Auto Scaling Group behind an ELB and one RDS (Relational Database Service) instance deployed with read replicas in the other AZ.
B. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 3 AZs with 2 EC2 instances in eachAZ inside an Auto Scaling Group behind an ELB and one RDS (Relational Database Service) Instance deployed with read replicas in the two other AZs.
C. A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 2 AZs with 3 EC2 instances m eachAZ inside an Auto Scaling Group behind an ELS and a Multi-AZ RDS (Relational Database Service) deployment.
D. A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ Inside an Auto Scaling Group behind an ELB (elastic load balancer). And an application tier deployed across 3 AZs with 2 EC2 instances ineach AZ inside an Auto Scaling Group behind an ELB and a Multi-AZ RDS (Relational Database services) deployment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS Multi-AZ Deployments
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.

Enhanced Durability

Multi-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. Multi-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL Server-native Mirroring 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 Multi-AZ deployments also extend to planned maintenance and backups. In the case of system upgrades like OS patching or DB Instance scaling, these operations are applied first on the standby, prior to the automatic failover. As a result, your availability impact is, again, only the time required for automatic failover to complete.

Unlike Single-AZ deployments, I/O activity is not suspended on your primary during backup for Multi-AZ deployments for the MySQL, 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 Multi-AZ deployments.

On instance failure in Amazon Aurora deployments, Amazon RDS uses RDS Multi-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.

QUESTION 45

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 individual file restores with a recovery time of no more than two hours. They have chosen to use RDS Oracle as the database.

Which backup architecture will meet these requirements?

A. Backup RDS using automated daily DB backups. Backup the EC2 instances using AMIs and supplement with file-level backup to S3 using traditional enterprise backup software to provide file level restore.

B. Backup RDS using a Multi-AZ Deployment. Backup the EC2 instances using Amis, and supplement by copying file system data to S3 to provide file level restore.

C. Backup RDS using automated daily DB backups. Backup the EC2 instances using EBS snapshots and supplement with file-level backups to Amazon Glacier using traditional enterprise backup software to provide file level restore.

D. Backup RDS database to S3 using Oracle RMAN. Backup the EC2 instances using Amis, and supplement with EBS snapshots for individual volume restore.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

Multi-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 (Multi-AZ).

QUESTION 46

Your company has HQ in Tokyo and branch offices all over the world and is using a logistics software with a multi-regional deployment on AWS in Japan, Europe and USA. The logistic software has a 3-tier architecture and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database.

In the HQ region you run an hourly batch process reading data from every region to compute cross-regional reports that are sent by email to all offices this batch process must be completed as fast as possible to quickly optimize logistics.

How do you build the database architecture in order to meet the requirements?

A. For each regional deployment, use RDS MySQL with a master in the region and a read replica in the HQ region

B. For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS snapshots to the HQ region

C. For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS snapshots to the HQ region

D. For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files hourly to the HQ regionE. Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network latency for the batch process

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 47
A web design company currently runs several FTP servers that their 250 customers use to upload and download large graphic files They wish to move this system to AWS to make it more scalable, but they wish to maintain customer privacy and Keep costs to a minimum.

What AWS architecture would you recommend?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
You would like to create a mirror image of your production environment in another region for disaster recovery purposes.

Which of the following AWS resources do not need to be recreated in the second region? (Choose 2 answers)

A. Route 53 Record Sets
B. IAM Roles
C. Elastic IP Addresses (EIP)
D. EC2 Key Pairs
E. Launch configurations
F. Security Groups

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
As per the document defined, new IPs should be reserved not the same ones
Elastic IP Addresses are static IP addresses designed for dynamic cloud computing. Unlike traditional static IP addresses, however, Elastic IP addresses enable you to mask instance or Availability Zone failures by programmatically remapping your public IP addresses to instances in your account in a particular region. For DR, you can also pre-allocate some IP addresses for the most critical systems so that their IP addresses are already known before disaster strikes. This can simplify the execution of the DR plan.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

QUESTION 49
Your company currently has a 2-tier web application running in an on-premises data center. You have experienced several infrastructure failures in the past two months resulting in significant financial losses. Your CIO is strongly agreeing to move the application to AWS. While working on achieving buy-in from the other company executives, he asks you to develop a disaster recovery plan to help improve Business continuity in the short term. He specifies a target Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour or less. He also asks you to implement the solution within 2 weeks.

Your database is 200GB in size and you have a 20Mbps Internet connection. How would you do this while minimizing costs?

A. Create an EBS backed private AMI which includes a fresh install of your application. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying theapplication across Multiple- Availability-Zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPN connection.

B. Deploy your application on EC2 instances within an Auto Scaling group across multiple availability zones. Asynchronously replicate transactions from your on-premises database to a database instance in AWS across a secure VPNconnection.

C. Create an EBS backed private AMI which includes a fresh install of your application. Setup a script in your data center to backup the local database every 1 hour and to encrypt and copy the resulting file to an S3 bucket using multi-part upload.

D. Install your application on a compute-optimized EC2 instance capable of supporting the application's average load. Synchronously replicate transactions from your on-premises database to a database instance in AWS across a secureDirect Connect connection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Overview of Creating Amazon EBS-Backed AMIs
First, launch an instance from an AMI that's similar to the AMI that you'd like to create. You can connect to your instance and customize it. When the instance is configured correctly, ensure data integrity by stopping the instance before you create an AMI, then create the image. When you create an Amazon EBS-backed AMI, we automatically register it for you.
Amazon EC2 powers down the instance before creating the AMI to ensure that everything on the instance is stopped and in a consistent state during the creation process. If you're confident that your instance is in a consistent state appropriate for AMI creation, you can tell Amazon EC2 not to power down and reboot the instance. Some file systems, such as XFS, can freeze and unfreeze activity, making it safe to create the image without rebooting the instance. During the AMI-creation process, Amazon EC2 creates snapshots of your instance's root volume and any other EBS volumes attached to your instance. If any volumes attached to the instance are encrypted, the new AMI only launches successfully on instances that support Amazon EBS encryption. For more information, see Amazon EBS Encryption.
Depending on the size of the volumes, it can take several minutes for the AMI-creation process to complete (sometimes up to 24 hours). You may find it more efficient to create snapshots of your volumes prior to creating your AMI. This way, only small, incremental snapshots need to be created when the AMI is created, and the process completes more quickly (the total time for snapshot creation remains the same). For more information, see Creating an Amazon EBS Snapshot.
After the process completes, you have a new AMI and snapshot created from the root volume of the instance. When you launch an instance using the new AMI, we create a new EBS volume for its root volume using the snapshot. Both the AMI and the snapshot incur charges to your account until you delete them. For more information, see Deregistering Your AMI.
If you add instance-store volumes or EBS volumes to your instance in addition to the root device volume, the block device mapping for the new AMI contains information for these volumes, and the block device mappings for instances that you launch from the new AMI automatically contain information for these volumes. The instance-store volumes specified in the block device mapping for the new instance are new and don't contain any data from the instance store volumes of the instance you used to create the AMI. The data on EBS volumes persists. For more information, see Block Device Mapping.

QUESTION 50
An enterprise wants to use a third-party SaaS application. The SaaS application needs to have access to issue several API commands to discover Amazon EC2 resources running within the enterprise's account The enterprise has internal security policies that require any outside access to their environment must conform to the principles of least privilege and there must be controls in place to ensure that the credentials used by the SaaS vendor cannot be used by any other third party.

Which of the following would meet all of these conditions?

A. From the AWS Management Console, navigate to the Security Credentials page and retrieve the access and secret key for your account.

B. Create an IAM user within the enterprise account assign a user policy to the IAM user that allows only the actions required by the SaaS application create a new access and secret key for the user and provide these credentials to theSaaS provider.

C. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.

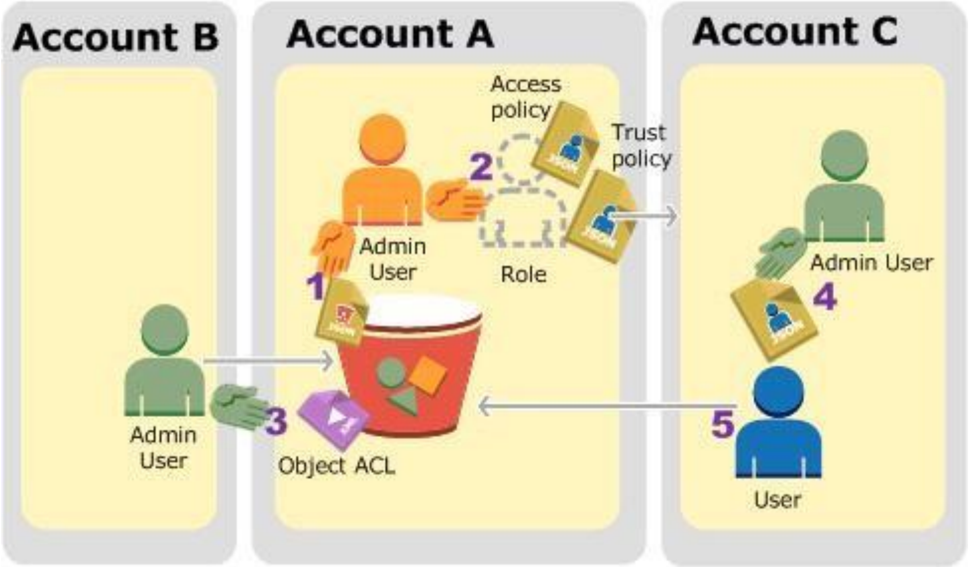
D. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required tor the SaaS application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

Correct Answer: C
Section: (none)
Explanation

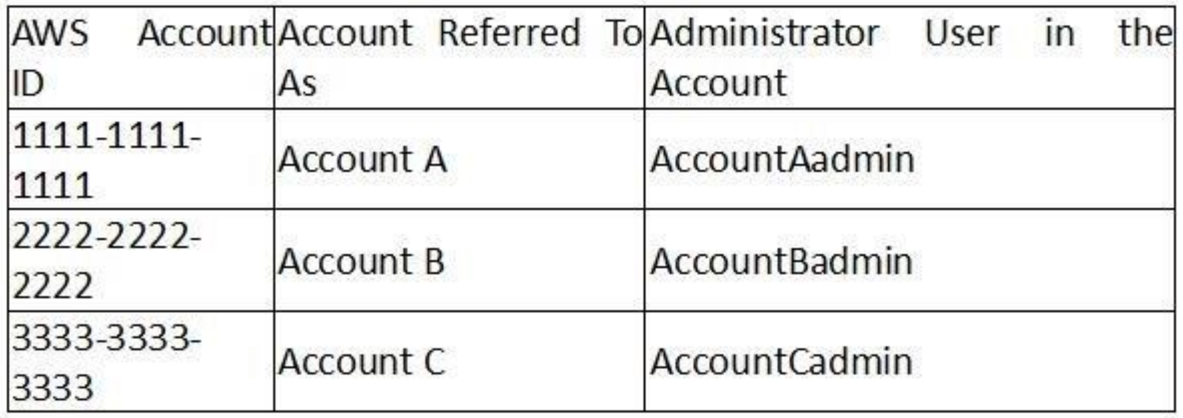
Explanation/Reference:
Explanation:
Granting Cross-account Permission to objects It Does Not Own
In this example scenario, you own a bucket and you have enabled other AWS accounts to upload objects. That is, your bucket can have objects that other AWS accounts own.
Now, suppose as a bucket owner, you need to grant cross-account permission on objects, regardless of who the owner is, to a user in another account. For example, that user could be a billing application that needs to access object metadata. There are two core issues:
The bucket owner has no permissions on those objects created by other AWS accounts. So for the bucket owner to grant permissions on objects it does not own, the object owner, the AWS account that created the objects, must first grant permission to the bucket owner. The bucket owner can then delegate those permissions.
Bucket owner account can delegate permissions to users in its own account but it cannot delegate permissions to other AWS accounts, because cross-account delegation is not supported.
In this scenario, the bucket owner can create an AWS Identity and Access Management (IAM) role with permission to access objects, and grant another AWS account permission to assume the role temporarily enabling it to access objects in the bucket.
Background: Cross-Account Permissions and Using IAM Roles
IAM roles enable several scenarios to delegate access to your resources, and cross-account access is one of the key scenarios. In this example, the bucket owner, Account A, uses an IAM role to temporarily delegate object access crossaccount to users in another AWS account, Account C. Each IAM role you create has two policies attached to it: A trust policy identifying another AWS account that can assume the role.

An access policy defining what permissions—for example, s3:GetObject—are allowed when someone assumes the role. For a list of permissions you can specify in a policy, see Specifying Permissions in a Policy. The AWS account identified in the trust policy then grants its user permission to assume the role. The user can then do the following to access objects:

Assume the role and, in response, get temporary security credentials.
Using the temporary security credentials, access the objects in the bucket.
For more information about IAM roles, go to Roles (Delegation and Federation) in IAM User Guide. The following is a summary of the walkthrough steps:



Account A administrator user attaches a bucket policy granting Account B conditional permission to upload objects.
Account A administrator creates an IAM role, establishing trust with Account C, so users in that account can access Account A. The access policy attached to the role limits what user in Account C can do when the user accesses Account A.
Account B administrator uploads an object to the bucket owned by Account A, granting full-control permission to the bucket owner.
Account C administrator creates a user and attaches a user policy that allows the user to assume the role.
User in Account C first assumes the role, which returns the user temporary security credentials. Using those temporary credentials, the user then accesses objects in the bucket.
For this example, you need three accounts. The following table shows how we refer to these accounts and the administrator users in these accounts. Per IAM guidelines (see About Using an Administrator User to Create Resources and Grant Permissions) we do not use the account root credentials in this walkthrough. Instead, you create an administrator user in each account and use those credentials in creating resources and granting them permissions



AWS Account ID	Account Referred To As	Administrator User in the Account
1111-1111-1111	Account A	AccountAadmin
2222-2222-2222	Account B	AccountBadmin
3333-3333-3333	Account C	AccountCadmin

QUESTION 51
A customer has a 10 GB AWS Direct Connect connection to an AWS region where they have a web application hosted on Amazon Elastic Computer Cloud (EC2). The application has dependencies on an on-premises mainframe database that uses a BASE (Basic Available, Soft state, Eventual consistency) rather than an ACID (Atomicity, Consistency, Isolation, Durability) consistency model. The application is exhibiting undesirable behavior because the database is not able to handle the volume of writes.

How can you reduce the load on your on-premises database resources in the most cost-effective way?

A. Use an Amazon Elastic Map Reduce (EMR) S3DistCp as a synchronization mechanism between the on-premises database and a Hadoop cluster on AWS.
B. Modify the application to write to an Amazon SQS queue and develop a worker process to flush the queue to the on-premises database.
C. Modify the application to use DynamoDB to feed an EMR cluster which uses a map function to write to the on-premises database.
D. Provision an RDS read-replica database on AWS to handle the writes and synchronize the two databases using Data Pipeline.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://aws.amazon.com/blogs/aws/category/amazon-elastic-map-reduce/

QUESTION 52
You are responsible for a legacy web application whose server environment is approaching end of life You would like to migrate this application to AWS as quickly as possible, since the application environment currently has the following limitations:

▪ The VM's single 10GB VMDK is almost full;
▪ Me virtual network interface still uses the 10Mbps driver, which leaves your 100Mbps WAN connection completely underutilized; ▪ It is currently running on a highly customized. Windows VM within a VMware environment; ▪ You do not have me installation media;

This is a mission critical application with an RTO (Recovery Time Objective) of 8 hours. RPO (Recovery Point Objective) of 1 hour.

How could you best migrate this application to AWS while meeting your business continuity requirements?

A. Use the EC2 VM Import Connector for vCenter to import the VM into EC2.
B. Use Import/Export to import the VM as an ESS snapshot and attach to EC2.
C. Use S3 to create a backup of the VM and restore the data into EC2.
D. Use me ec2-bundle-instance API to Import an Image of the VM into EC2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
An AWS customer runs a public blogging website. The site users upload two million blog entries a month. The average blog entry size is 200 KB. The access rate to blog entries drops to negligible 6 months after publication and users rarely access a blog entry 1 year after publication. Additionally, blog entries have a high update rate during the first 3 months following publication, this drops to no updates after 6 months. The customer wants to use CloudFront to improve his user's load times.

Which of the following recommendations would you make to the customer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
You are implementing a URL whitelisting system for a company that wants to restrict outbound HTTP'S connections to specific domains from their EC2-hosted applications. You deploy a single EC2 instance running proxy software and configure It to accept traffic from all subnets and EC2 instances in the VPC. You configure the proxy to only pass through traffic to domains that you define in its whitelist configuration. You have a nightly maintenance window or 10 minutes where all instances fetch new software updates. Each update Is about 200MB In size and there are 500 instances In the VPC that routinely fetch updates. After a few days you notice that some machines are failing to successfully download some, but not all of their updates within the maintenance window. The download URLs used for these updates are correctly listed in the proxy's whitelist configuration and you are able to access them manually using a web browser on the instances.

What might be happening? (Choose 2)

A. You are running the proxy on an undersized EC2 instance type so network throughput is not sufficient for all instances to download their updates in time.
B. You are running the proxy on a sufficiently-sized EC2 instance in a private subnet and its network throughput is being throttled by a NAT running on an undersized EC2 instance.
C. The route table for the subnets containing the affected EC2 instances is not configured to direct network traffic for the software update locations to the proxy.
D. You have not allocated enough storage to the EC2 instance running the proxy so the network buffer is filling up, causing some requests to fail.
E. You are running the proxy in a public subnet but have not allocated enough EIPs to support the needed network throughput through the Internet Gateway (IGW).

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

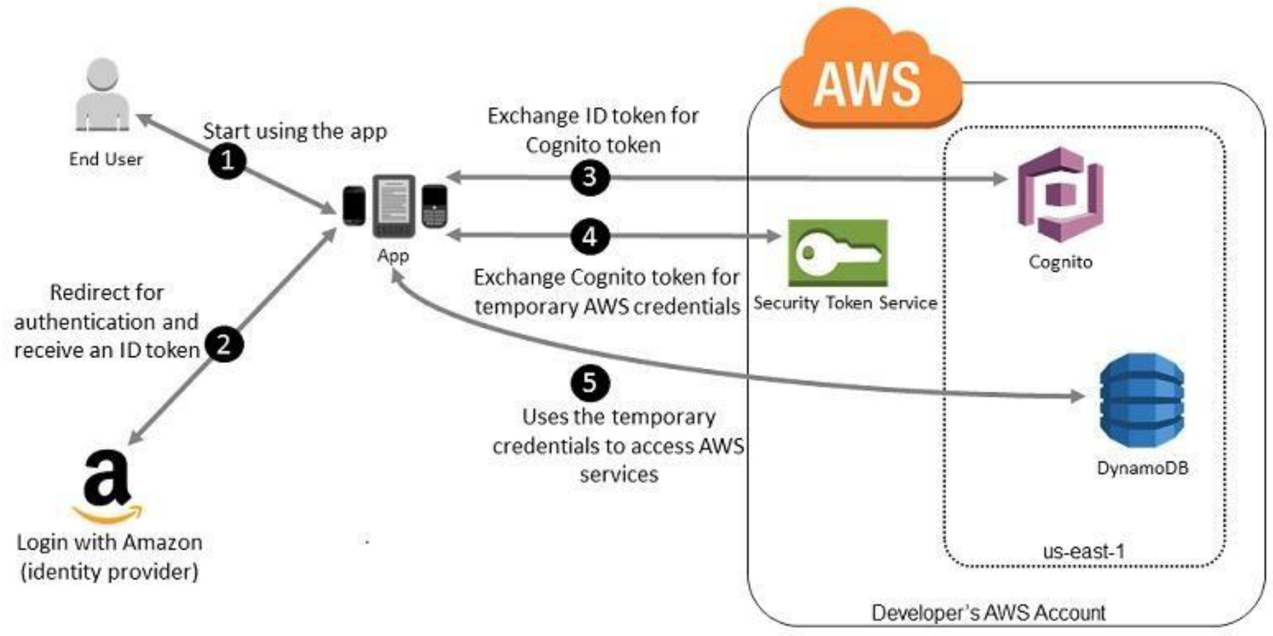
QUESTION 55
Company B is launching a new game app for mobile devices. Users will log into the game using their existing social media account to streamline data capture. Company B would like to directly save player data and scoring information from the mobile app to a DynamoDS table named Score Data When a user saves their game the progress data will be stored to the Game state S3 bucket.

What is the best approach for storing data to DynamoDB and S3?

A. Use an EC2 Instance that is launched with an EC2 role providing access to the Score Data DynamoDB table and the GameState S3 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 S3 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 S3 bucket.
D. Use an IAM user with access credentials assigned a role providing access to the Score Data DynamoDB table and the Game State S3 bucket for distribution with the mobile app.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 S3 and DynamoDB.
When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app.
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 long-term 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 Mobile 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 AssumeRoleWithWebIdentity 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 Mobile 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 S3 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 ID with her chosen IdPs. She also configures the application with each of these providers. In her AWS account that contains the Amazon S3 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 trust 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. Adele's app can trade this authentication information for a set of temporary security credentials that consist of an AWS access key ID, 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


AWS
End User
Start using the app
1
App
Exchange ID token for Cognito token
3
Cognito
4
Exchange Cognito token for temporary AWS credentials
Security Token Service
Redirect for authentication and receive an ID token
2
5
Uses the temporary credentials to access AWS services
DynamoDB
Login with Amazon (identity provider)
us-east-1
Developer's AWS Account

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 ID 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 Management 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 roles 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.

QUESTION 56
Your company is getting ready to do a major public announcement of a social media site on AWS. The website is running on EC2 instances deployed across multiple Availability Zones with a Multi-AZ RDS MySQL Extra Large DB Instance. The site performs a high number of small reads and writes per second and relies on an eventual consistency model. After comprehensive tests you discover that there is read contention on RDS MySQL.

Which are the best approaches to meet these requirements? (Choose 2 answers)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

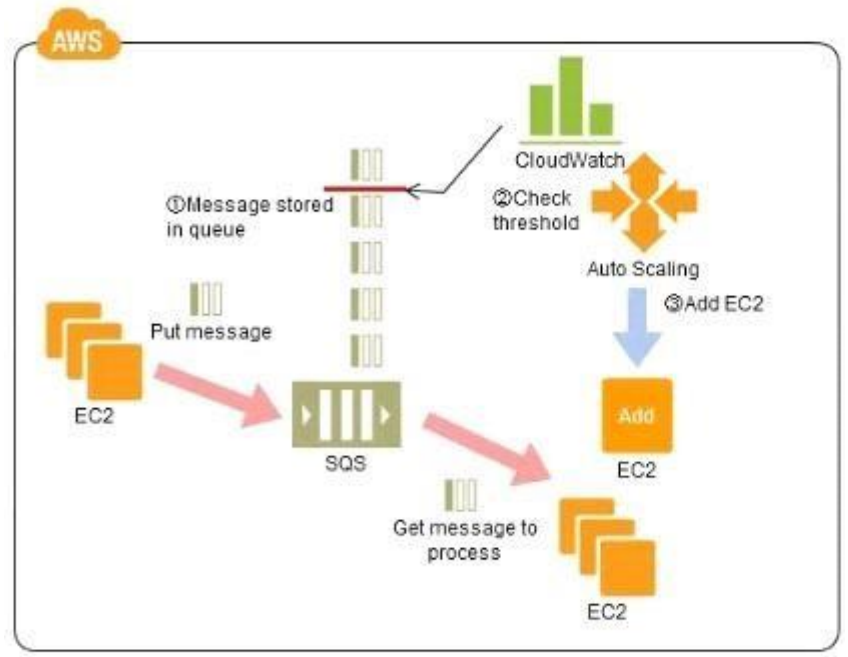
QUESTION 57
You are designing an intrusion detection prevention (IDS/IPS) solution for a customer web application in a single VPC. You are considering the options for implementing IOS IPS protection for traffic coming from the Internet.
Which of the following options would you consider? (Choose 2 answers)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
EC2 does not allow promiscuous mode, and you cannot put something in between the ELB and the web server (like a listener or IDP)

QUESTION 58



Refer to the architecture diagram above of a batch processing solution using Simple Queue Service (SQS) to set up a message queue between EC2 instances which are used as batch processors Cloud Watch monitors the number of Job requests (queued messages) and an Auto Scaling group adds or deletes batch servers automatically based on parameters set in Cloud Watch alarms.

You can use this architecture to implement which of the following features in a cost effective and efficient manner?

A. Reduce the overall lime for executing jobs through parallel processing by allowing a busy EC2 instance that receives a message to pass it to the next instance in a daisy-chain setup.
B. Implement fault tolerance against EC2 instance failure since messages would remain in SQS and worn can continue with recovery of EC2 instances implement fault tolerance against SQS failure by backing up messages to S3.
C. Implement message passing between EC2 instances within a batch by exchanging messages through SQS.
D. Coordinate number of EC2 instances with number of job requests automatically thus Improving cost effectiveness.
E. Handle high priority jobs before lower priority jobs by assigning a priority metadata field to SQS messages.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are cases where a large number of batch jobs may need processing, and where the jobs may need to be re-prioritized.
For example, one such case is one where there are differences between different levels of services for unpaid users versus subscriber users (such as the time until publication) in services enabling, for example, presentation files to be uploaded for publication from a web browser. When the user uploads a presentation file, the conversion processes, for example, for publication are performed as batch processes on the system side, and the file is published after the conversion. Is it then necessary to be able to assign the level of priority to the batch processes for each type of subscriber?
Explanation of the Cloud Solution/Pattern

A queue is used in controlling batch jobs. The queue need only be provided with priority numbers. Job requests are controlled by the queue, and the job requests in the queue are processed by a batch server. In Cloud computing, a highly reliable queue is provided as a service, which you can use to structure a highly reliable batch system with ease. You may prepare multiple queues depending on priority levels, with job requests put into the queues depending on their priority levels, to apply prioritization to batch processes. The performance (number) of batch servers corresponding to a queue must be in accordance with the priority level thereof.

Implementation

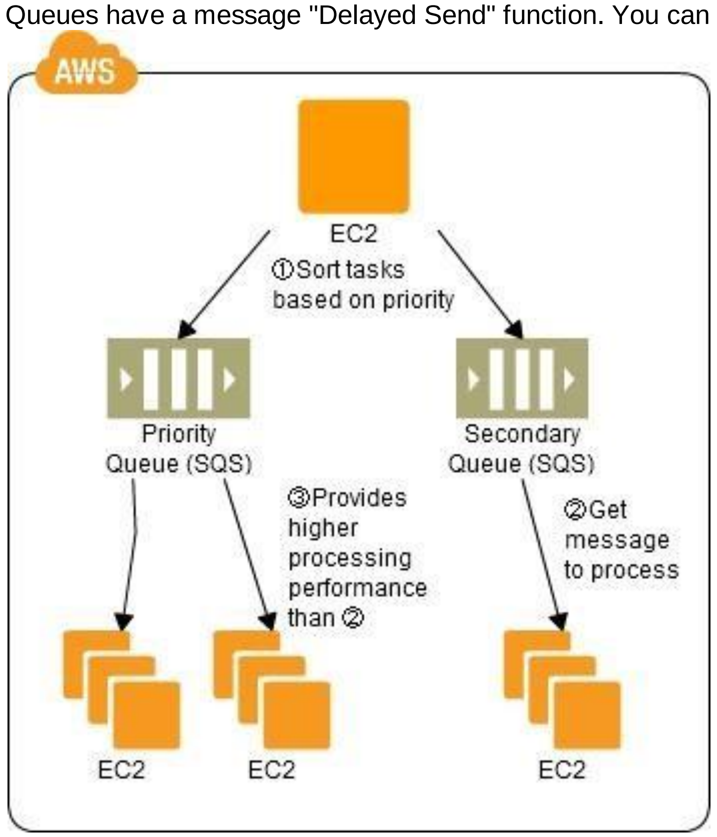
In AWS, the queue service is the Simple Queue Service (SQS). Multiple SQS queues may be prepared to prepare queues for individual priority levels (with a priority queue and a secondary queue). Moreover, you may also use the message Delayed Send function to delay process execution.

Use SQS to prepare multiple queues for the individual priority levels.

Place those processes to be executed immediately (job requests) in the high priority queue.

Prepare numbers of batch servers, for processing the job requests of the queues, depending on the priority levels.

Queues have a message "Delayed Send" function. You can use this to delay the time for starting a process. Configuration



Benefits

You can increase or decrease the number of servers for processing jobs to change automatically the processing speeds of the priority queues and secondary queues.

You can handle performance and service requirements through merely increasing or decreasing the number of EC2 instances used in job processing.

Even if an EC2 were to fail, the messages (jobs) would remain in the queue service, enabling processing to be continued immediately upon recovery of the EC2 instance, producing a system that is robust to failure.

Cautions

Depending on the balance between the number of EC2 instances for performing the processes and the number of messages that are queued, there may be cases where processing in the secondary queue may be completed first, so you need to monitor the processing speeds in the primary queue and the secondary queue.

QUESTION 59

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

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

Which design would you choose to meet these requirements?

A. Use AWS data Pipeline to schedule a DynamoDB cross region copy once a day, create a “Lastupdated” attribute in your DynamoDB table that would represent the timestamp of the last update and use it as a filter.

B. Use EMR and write a custom script to retrieve data from DynamoDB in the current region using a SCAN operation and push it to DynamoDB in the second region.

C. Use AWS data Pipeline to schedule an export of the DynamoDB table to S3 in the current region once a day then schedule another task immediately after it that will import data from S3 to DynamoDB in the other region.

D. Send also each Ante into an SQS queue in me second region; use an auto-scaling group behind the SQS queue to replay the write in the second region.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60
You are designing a social media site and are considering how to mitigate distributed denial-of-service (DDoS) attacks.

Which of the below are viable mitigation techniques? (Choose 3)

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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61 You must architect the migration of a web application to AWS. The application consists of Linux web servers running a custom web server. You are required to save the logs generated from the application to a durable location.

What options could you select to migrate the application to AWS? (Choose 2)

A. Create an AWS Elastic Beanstalk application using the custom web server platform. Specify the web server executable and the application project and source files. Enable log file rotation to Amazon Simple Storage Service (S3).
B. Create Dockerfile for the application. Create an AWS OpsWorks stack consisting of a custom layer. Create custom recipes to install Docker and to deploy your Docker container using the Dockerfile. Create customer recipes to installand configure the application to publish the logs to Amazon CloudWatch Logs.
C. Create Dockerfile for the application. Create an AWS OpsWorks stack consisting of a Docker layer that uses the Dockerfile. Create custom recipes to install and configure Amazon Kineses to publish the logs into Amazon CloudWatch.D. Create a Dockerfile for the application. Create an AWS Elastic Beanstalk application using the Docker platform and the Dockerfile. Enable logging the Docker configuration to automatically publish the application logs. Enable log file rotation to Amazon S3.
E. Use VM import/Export to import a virtual machine image of the server into AWS as an AMI. Create an Amazon Elastic Compute Cloud (EC2) instance from AMI, and install and configure the Amazon CloudWatch Logs agent. Create a new AMI from the instance. Create an AWS Elastic Beanstalk application using the AMI platform and the new AMI.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A web company is looking to implement an external payment service into their highly available application deployed in a VPC Their application EC2 instances are behind a public facing ELB. Auto scaling is used to add additional instances as traffic increases under normal load the application runs 2 instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisting IP addresses are allowed at a time and can be added through an API.

How should they architect their solution?

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 63
Your website is serving on-demand training videos to your workforce. Videos are uploaded monthly in high resolution MP4 format. Your workforce is distributed globally often on the move and using company-provided tablets that require the HTTP Live Streaming (HLS) protocol to watch a video. Your company has no video transcoding expertise and it required you may need to pay for a consultant.

How do you implement the most cost-efficient architecture without compromising high availability and quality of video delivery?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64 A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

A. AWS RDS
B. AWS ELB
C. AWS Route53
D. AWS EMR

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, EC2, Auto Scaling, ELB, and Route 53 can provide the monitoring data every minute.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION 65
A customer has established an AWS Direct Connect connection to AWS. The link is up and routes are being advertised from the customer's end, however the customer is unable to connect from EC2 instances inside its VPC to servers residing in its datacenter.

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

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 66

You are running a news website in the eu-west-1 region that updates every 15 minutes. The website has a world-wide audience. It uses an Auto Scaling group behind an Elastic Load Balancer and an Amazon RDS database. Static content resides on Amazon S3, and is distributed through Amazon CloudFront. Your Auto Scaling group is set to trigger a scale up event at 60% CPU utilization. You use an Amazon RDS extra large DB instance with 10.000 Provisioned IOPS, its CPU utilization is around 80%, while freeable memory is in the 2 GB range.

Web analytics reports show that the average load time of your web pages is around 1.5 to 2 seconds, but your SEO consultant wants to bring down the average load time to under 0.5 seconds. How

would you improve page load times for your users? (Choose 3 answers)

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an IPSec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user.

Which two approaches can satisfy these objectives? (Choose 2)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Imagine that in your organization, you want to provide a way for users to copy data from their computers to a backup folder. You build an application that users can run on their computers. On the back end, the application reads and writes objects in an S3 bucket. Users don't have direct access to AWS. Instead, the application communicates with an identity provider (IdP) to authenticate the user. The IdP gets the user information from your organization's identity store (such as an LDAP directory) and then generates a SAML assertion that includes authentication and authorization information about that user. The application then uses that assertion to make a call to the AssumeRoleWithSAML API to get temporary security credentials. The app can then use those credentials to access a folder in the S3 bucket that's specific to the user. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

QUESTION 68
Your company previously configured a heavily used, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and would like to start using the new connection.

After configuring DirectConnect settings in the AWS Console, which of the following options win provide the most seamless transition for your users?

A. Delete your existing VPN connection to avoid routing loops configure your DirectConnect router with the appropriate settings and verity network traffic is leveraging DirectConnect.
B. Configure your DirectConnect router with a higher BGP priority man your VPN router, verify network traffic is leveraging Directconnect and then delete your existing VPN connection.
C. Update your VPC route tables to point to the DirectConnect connection configure your DirectConnect router with the appropriate settings verify network traffic is leveraging DirectConnect and then delete the VPN connection.
D. Configure your DirectConnect router, update your VPC route tables to point to the DirectConnect connection, configure your VPN connection with a higher BGP priority, and verify network traffic is leveraging the DirectConnect

connection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q. Can I use AWS Direct Connect and a VPN Connection to the same VPC simultaneously?
Yes. However, only in fail-over scenarios. The Direct Connect path will always be preferred, when established, regardless of AS path prepending. https://aws.amazon.com/directconnect/faqs/

QUESTION 69
Your company hosts a social media website for storing and sharing documents. The web application allows user to upload large files while resuming and pausing the upload as needed. Currently, files are uploaded to your PHP front end backed by Elastic Load Balancing and an autoscaling fleet of Amazon Elastic Compute Cloud (EC2) instances that scale upon average of bytes received (NetworkIn). After a file has been uploaded, it is copied to Amazon Simple Storage Service (S3). Amazon EC2 instances use an AWS Identity and Access Management (IAM) role that allows Amazon S3 uploads. Over the last six months, your user base and scale have increased significantly, forcing you to increase the Auto Scaling group's Max parameter a few times. Your CFO is concerned about rising costs and has asked you to adjust the architecture where needed to better optimize costs.

Which architecture change could you introduce to reduce costs and still keep your web application secure and scalable?

A. Replace the Auto Scaling launch configuration to include c3.8xlarge instances; those instances can potentially yield a network throuthput of 10gbps.
B. Re-architect your ingest pattern, have the app authenticate against your identity provider, and use your identity provider as a broker fetching temporary AWS credentials from AWS Secure Token Service (GetFederationToken). Securelypass the credentials and S3 endpoint/prefix to your app. Implement client-side logic to directly upload the file to Amazon S3 using the given credentials and S3 prefix.
C. Re-architect your ingest pattern, and move your web application instances into a VPC public subnet. Attach a public IP address for each EC2 instance (using the Auto Scaling launch configuration settings). Use Amazon Route 53 RoundRobin records set and HTTP health check to DNS load balance the app requests; this approach will significantly reduce the cost by bypassing Elastic Load Balancing.
D. Re-architect your ingest pattern, have the app authenticate against your identity provider, and use your identity provider as a broker fetching temporary AWS credentials from AWS Secure Token Service (GetFederationToken). Securelypass the credentials and S3 endpoint/prefix to your app. Implement client-side logic that used the S3 multipart upload API to directly upload the file to Amazon S3 using the given credentials and S3 prefix.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
You require the ability to analyze a customer's clickstream data on a website so they can do behavioral analysis. Your customer needs to know what sequence of pages and ads their customer clicked on. This data will be used in real time to modify the page layouts as customers click through the site to increase stickiness and advertising click-through.

Which option meets the requirements for captioning and analyzing this data?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://www.slideshare.net/AmazonWebServices/aws-webcast-introduction-to-amazon-kinesis

QUESTION 71
You have deployed a three-tier web application in a VPC with a CIDR block of 10.0.0.0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance tor a total of seven EC2 instances. The web, application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS Web (raffle gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load unfortunately some of these new instances fail to launch.

Which of the following could be the root caused? (Choose 2 answers)

A. AWS reserves the first and the last private IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances
B. The Internet Gateway (IGW) of your VPC has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
C. The ELB has scaled-up, adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches
D. AWS reserves one IP address in each subnet's CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances
E. AWS reserves the first four and the last IP address in each subnet's CIDR block so you do not have enough addresses left to launch all of the new EC2 instances

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Your company produces customer commissioned one-of-a-kind skiing helmets combining nigh fashion with custom technical enhancements Customers can show off their Individuality on the ski slopes and have access to head-up-displays. GPS rear-view cams and any other technical innovation they wish to embed in the helmet.
The current manufacturing process is data rich and complex including assessments to ensure that the custom electronics and materials used to assemble the helmets are to the highest standards Assessments are a mixture of human and automated assessments you need to add a new set of assessment to model the failure modes of the custom electronics using GPUs with CUDA, across a cluster of servers with low latency networking.

What architecture would allow you to automate the existing process using a hybrid approach and ensure that the architecture can support the evolution of processes over time?

A. Use AWS Data Pipeline to manage movement of data & meta-data and assessments Use an auto-scaling group of G2 instances in a placement group.
B. Use Amazon Simple Workflow (SWF) to manages assessments, movement of data & meta-data Use an auto-scaling group of G2 instances in a placement group.
C. Use Amazon Simple Workflow (SWF) to manages assessments movement of data & meta-data Use an auto-scaling group of C3 instances with SR-IOV (Single Root I/O Virtualization).
D. Use AWS data Pipeline to manage movement of data & meta-data and assessments use auto-scaling group of C3 with SR-IOV (Single Root I/O virtualization).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
You are designing an SSL/TLS solution that requires HTTPS clients to be authenticated by the Web server using client certificate authentication. The solution must be resilient. Which

of the following options would you consider for configuring the web server infrastructure? (Choose 2)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
You are migrating a legacy client-server application to AWS. The application responds to a specific DNS domain (e.g. www.example.com) and has a 2-tier architecture, with multiple application servers and a database server. Remote clients use TCP to connect to the application servers. The application servers need to know the IP address of the clients in order to function properly and are currently taking that information from the TCP socket. A Multi-AZ RDS MySQL instance will be used for the database.
During the migration you can change the application code, but you have to file a change request.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
You are designing a personal document-archiving solution for your global enterprise with thousands of employee. Each employee has potentially gigabytes of data to be backed up in this archiving solution. The solution will be exposed to the employees as an application, where they can just drag and drop their files to the archiving system. Employees can retrieve their archives through a web interface. The corporate network has high bandwidth AWS Direct Connect connectivity to AWS.
You have a regulatory requirement that all data needs to be encrypted before being uploaded to the cloud.

How do you implement this in a highly available and cost-efficient way?

A. Manage encryption keys on-premises in an encrypted relational database. Set up an on-premises server with sufficient storage to temporarily store files, and then upload them to Amazon S3, providing a client-side master key.
B. Mange encryption keys in a Hardware Security Module (HSM) appliance on-premises serve r with sufficient storage to temporarily store, encrypt, and upload files directly into Amazon Glacier.
C. Manage encryption keys in Amazon Key Management Service (KMS), upload to Amazon Simple Storage Service (S3) with client-side encryption using a KMS customer master key ID, and configure Amazon S3 lifecycle policies to storeeach object using the Amazon Glacier storage tier.
D. Manage encryption keys in an AWS CloudHSM appliance. Encrypt files prior to uploading on the employee desktop, and then upload directly into Amazon Glacier.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A company is building a voting system for a popular TV show, viewers win watch the performances then visit the show's website to vote for their favorite performer. It is expected that in a short period of time after the show has finished the site will receive millions of visitors. The visitors will first login to the site using their Amazon.com credentials and then submit their vote. After the voting is completed the page will display the vote totals. The company needs to build the site such that can handle the rapid influx of traffic while maintaining good performance but also wants to keep costs to a minimum.

Which of the design patterns below should they use?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 77
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your servers on-premises will be communicating with your VPC instances. You will be establishing IPSec tunnels over the Internet You will be using VPN gateways, and terminating the IPSec tunnels on AWS supported customer gateways.

Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? (Choose 4 answers)

A. End-to-end protection of data in transit
B. End-to-end Identity authentication
C. Data encryption across the Internet
D. Protection of data in transit over the Internet
E. Peer identity authentication between VPN gateway and customer gateway
F. Data integrity protection across the Internet

Correct Answer: CDEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
You are responsible for a web application that consists of an Elastic Load Balancing (ELB) load balancer in front of an Auto Scaling group of Amazon Elastic Compute Cloud (EC2) instances. For a recent deployment of a new version of the application, a new Amazon Machine Image (AMI) was created, and the Auto Scaling group was updated with a new launch configuration that refers to this new AMI. During the deployment, you received complaints from users that the website was responding with errors. All instances passed the ELB health checks.

What should you do in order to avoid errors for future deployments? (Choose 2)

A. Add an Elastic Load Balancing health check to the Auto Scaling group. Set a short period for the health checks to operate as soon as possible in order to prevent premature registration of the instance to the load balancer.
B. Enable EC2 instance CloudWatch alerts to change the launch configuration's AMI to the previous one. Gradually terminate instances that are using the new AMI.
C. Set the Elastic Load Balancing health check configuration to target a part of the application that fully tests application health and returns an error if the tests fail.
D. Create a new launch configuration that refers to the new AMI, and associate it with the group. Double the size of the group, wait for the new instances to become healthy, and reduce back to the original size. If new instances do notbecome healthy, associate the previous launch configuration.
E. Increase the Elastic Load Balancing Unhealthy Threshold to a higher value to prevent an unhealthy instance from going into service behind the load balancer.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which is a valid Amazon Resource name (ARN) for IAM?

A. aws:iam::123456789012:instance-profile/Webserver
B. arn:aws:iam::123456789012:instance-profile/Webserver
C. 123456789012:aws:iam::instance-profile/Webserver
D. arn:aws:iam::123456789012::instance-profile/Webserver

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IAM ARNs
Most resources have a friendly name (for example, a user named Bob or a group named Developers). However, the access policy language requires you to specify the resource or resources using the following Amazon Resource Name (ARN) format. arn:aws:service:region:account:resource
Where: service identifies the AWS product. For IAM resources, this is always iam.
region is the region the resource resides in. For IAM resources, this is always left blank.
account is the AWS account ID with no hyphens (for example, 123456789012).
resource is the portion that identifies the specific resource by name.

You can use ARNs in IAM for users (IAM and federated), groups, roles, policies, instance profiles, virtual MFA devices, and server certificates. The following table shows the ARN format for each and an example. The region portion of the ARN is blank because IAM resources are global.

QUESTION 80

Dave is the main administrator in Example Corp., and he decides to use paths to help delineate the users in the company and set up a separate administrator group for each path-based division. Following is a subset of the full list of paths he plans to use:

• /marketing
• /sales
• /legal

Dave creates an administrator group for the marketing part of the company and calls it Marketing_Admin.
He assigns it the /marketing path. The group's ARN is arn:aws:iam::123456789012:group/marketing/Marketing_Admin.
Dave assigns the following policy to the Marketing_Admin group that gives the group permission to use all IAM actions with all groups and users in the /marketing path. The policy also gives the Marketing_Admin group permission to perform any AWS S3 actions on the objects in the portion of the corporate bucket.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Deny",
"Action": "iam:*",
"Resource": [
"arn:aws:iam::123456789012:group/marketing/*",
"arn:aws:iam::123456789012:user/marketing/*"
]
},
{
"Effect": "Allow",
"Action": "s3:*",
"Resource": "arn:aws:s3:::example_bucket/marketing/*"
},
{
"Effect": "Allow",
"Action": "s3:ListBucket*",
"Resource": "arn:aws:s3:::example_bucket",
"Condition":{"StringLike":{"s3:prefix": "marketing/*"}}
}
]
}
```

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Effect Deny

QUESTION 81

Your fortune 500 company has under taken a TCO analysis evaluating the use of Amazon S3 versus acquiring more hardware The outcome was that ail employees would be granted access to use Amazon S3 for storage of their personal documents.

Which of the following will you need to consider so you can set up a solution that incorporates single sign-on from your corporate AD or LDAP directory and restricts access for each user to a designated user folder in a bucket? (Choose 3)

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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A company is running a batch analysis every hour on their main transactional DB, running on an RDS MySQL instance, to populate their central Data Warehouse running on Redshift. During the execution of the batch, their transactional applications are very slow. When the batch completes they need to update the top management dashboard with the new data. The dashboard is produced by another system running on-premises that is currently started when a manuallysent email notifies that an update is required. The on-premises system cannot be modified because is managed by another team.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
You are running a successful multitier web application on AWS and your marketing department has asked you to add a reporting tier to the application. The reporting tier will aggregate and publish status reports every 30 minutes from usergenerated information that is being stored in your web application s database. You are currently running a Multi-AZ RDS MySQL instance for the database tier. You also have implemented Elasticache as a database caching layer between the application tier and database tier.

Please select the answer that will allow you to successfully implement the reporting tier with as little impact as possible to your database.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS allows you to use read replicas with Multi-AZ deployments. In Multi-AZ deployments for MySQL, Oracle, SQL Server, and PostgreSQL, the data in your primary DB Instance is synchronously replicated to to a standby instance in a different Availability Zone (AZ). Because of their synchronous replication, Multi-AZ deployments for these engines offer greater data durability benefits than do read replicas. (In all Amazon RDS for Aurora deployments, your data is automatically replicated across 3 Availability Zones.)
You can use Multi-AZ deployments and read replicas in conjunction to enjoy the complementary benefits of each. You can simply specify that a given Multi-AZ deployment is the source DB Instance for your Read replicas. That way you gain both the data durability and availability benefits of Multi-AZ deployments and the read scaling benefits of read replicas.
Note that for Multi-AZ deployments, you have the option to create your read replica in an AZ other than that of the primary and the standby for even more redundancy. You can identify the AZ corresponding to your standby by looking at the "Secondary Zone" field of your DB Instance in the AWS Management Console.

QUESTION 84
You are designing a data leak prevention solution for your VPC environment. You want your VPC Instances to be able to access software depots and distributions on the Internet for product updates. The depots and distributions are accessible via third party CDNs by their URLs.
You want to explicitly deny any other outbound connections from your VPC instances to hosts on the internet.

Which of the following options would you consider?

A. Configure a web proxy server in your VPC and enforce URL-based rules for outbound access Remove default routes.
B. Implement security groups and configure outbound rules to only permit traffic to software depots.
C. Move all your instances into private VPC subnets remove default routes from all routing tables and add specific routes to the software depots and distributions only.
D. Implement network access control lists to all specific destinations, with an Implicit deny all rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85 You have an application running on an EC2 instance which will allow users to download files from a private S3 bucket using a pre-signed URL. Before generating the URL, the application should verify the existence of the file in S3.

How should the application use AWS credentials to access the S3 bucket securely?

A. Use the AWS account access keys; the application retrieves the credentials from the source code of the application.
B. Create an IAM role for EC2 that allows list access to objects In the S3 bucket; launch the Instance with the role, and retrieve the role's credentials from the EC2 instance metadata.
C. Create an IAM user for the application with permissions that allow list access to the S3 bucket; the application retrieves the 1AM user credentials from a temporary directory with permissions that allow read access only to the Application user.
D. Create an IAM user for the application with permissions that allow list access to the S3 bucket; launch the instance as the IAM user, and retrieve the IAM user's credentials from the EC2 instance user data.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Your system recently experienced down time during the troubleshooting process. You found that a new administrator mistakenly terminated several production EC2 instances.

Which of the following strategies will help prevent a similar situation in the future?

The administrator still must be able to: ▪ launch, start stop, and terminate development resources. ▪ launch and start production instances.

A. Create an IAM user, which is not allowed to terminate instances by leveraging production EC2 termination protection.
B. Leverage resource based tagging, along with an IAM user which can prevent specific users from terminating production, EC2 resources.
C. Leverage EC2 termination protection and multi-factor authentication, which together require users to authenticate before terminating EC2 instances
D. Create an IAM user and apply an IAM role which prevents users from terminating production EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Working with volumes
When an API action requires a caller to specify multiple resources, you must create a policy statement that allows users to access all required resources. If you need to use a Condition element with one or more of these resources, you must create multiple statements as shown in this example.
The following policy allows users to attach volumes with the tag "volume_user=iam-user-name" to instances with the tag "department=dev", and to detach those volumes from those instances. If you attach this policy to an IAM group, the aws:username policy variable gives each IAM user in the group permission to attach or detach volumes from the instances with a tag named volume_user that has his or her IAM user name as a value.

```
{
   "Version": "2012-10-17",
   "Statement": [{
    "Effect": "Allow",
    "Action": [
     "ec2:AttachVolume",
     "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
    "Condition": {
     "StringEquals": {
      "ec2:ResourceTag/department": "dev"
     }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
     "ec2:AttachVolume",
     "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
    "Condition": {
     "StringEquals": {
      "ec2:ResourceTag/volume_user": "${aws:username}"
     }
    }
  }
 ]
}
```

Launching instances (RunInstances)

The RunInstances API action launches one or more instances. RunInstances requires an AMI and creates an instance; and users can specify a key pair and security group in the request. Launching into EC2-VPC requires a subnet, and creates a network interface. Launching from an Amazon EBS-backed AMI creates a volume. Therefore, the user must have permission to use these Amazon EC2 resources. The caller can also configure the instance using optional parameters to RunInstances, such as the instance type and a subnet. You can create a policy statement that requires users to specify an optional parameter, or restricts users to particular values for a parameter. The examples in this section demonstrate some of the many possible ways that you can control the configuration of an instance that a user can launch.

Note that by default, users don't have permission to describe, start, stop, or terminate the resulting instances. One way to grant the users permission to manage the resulting instances is to create a specific tag for each instance, and then create a statement that enables them to manage instances with that tag. For more information, see 2: Working with instances. a. AMI

The following policy allows users to launch instances using only the AMIs that have the specified tag, "department=dev", associated with them. The users can't launch instances using other AMIs because the Condition element of the first statement requires that users specify an AMI that has this tag. The users also can't launch into a subnet, as the policy does not grant permissions for the subnet and network interface resources. They can, however, launch into EC2-Classic. The second statement uses a wildcard to enable users to create instance resources, and requires users to specify the key pair project_keypair and the security group sg-1a2b3c4d. Users are still able to launch instances without a key pair.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/project_keypair",
          "arn:aws:ec2:region:account:security-group/sg-1a2b3c4d"
        ]
      }
   ]
}
```

Alternatively, the following policy allows users to launch instances using only the specified AMIs, ami-9e1670f7 and ami-45cf5c3c. The users can't launch an instance using other AMIs (unless another statement grants the users permission to do so), and the users can't launch an instance into a subnet.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account:instance/*",
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:key-pair/*",
        "arn:aws:ec2:region:account:security-group/*"
      ]
    }
   ]
}
```

Alternatively, the following policy allows users to launch instances from all AMIs owned by Amazon. The Condition element of the first statement tests whether ec2:Owner is amazon. The users can't launch an instance using other AMIs (unless another statement grants the users permission to do so). The users are able to launch an instance into a subnet.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
            }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account:instance/*",
         "arn:aws:ec2:region:account:subnet/*",
         "arn:aws:ec2:region:account:volume/*",
         "arn:aws:ec2:region:account:network-interface/*",
         "arn:aws:ec2:region:account:key-pair/*",
         "arn:aws:ec2:region:account:security-group/*"
         ]
      }
   ]
}
```

b. Instance type

The following policy allows users to launch instances using only the t2.micro or t2.small instance type, which you might do to control costs. The users can't launch larger instances because the Condition element of the first statement tests whether ec2:InstanceType is either t2.micro or t2.small.

```
{
   "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

Alternatively, you can create a policy that denies users permission to launch any instances except t2.micro and t2.small instance types.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

c. Subnet

The following policy allows users to launch instances using only the specified subnet, subnet-12345678. The group can't launch instances into any another subnet (unless another statement grants the users permission to do so). Users are still able to launch instances into EC2-Classic.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:subnet/subnet-12345678",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
    ]
   }
  ]
}
```

Alternatively, you could create a policy that denies users permission to launch an instance into any other subnet. The statement does this by denying permission to create a network interface, except where subnet subnet-12345678 is specified. This denial overrides any other policies that are created to allow launching instances into other subnets. Users are still able to launch instances into EC2-Classic.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:network-interface/*"
    ],
    "Condition": {
      "ArnNotEquals": {
        "ec2:Subnet": "arn:aws:ec2:region:account:subnet/subnet-12345678"
        }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

QUESTION 87

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

Which AWS storage and database architecture meets the requirements of the application?

A. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more readreplicas. Backup: web servers, app servers, and database backed up weekly to Glacier using snapshots.
B. Web servers: store read-only data in an EC2 NFS server; mount to each web server at boot time. App servers: share state using a combination of DynamoDB and IP multicast. Database: use RDS with multi-AZ deployment and one ormore Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
C. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more ReadReplicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
D. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment. Backup: web and appservers backed up weekly via AMIs, database backed up via DB snapshots.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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
Multi-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. Multi-AZ deployments for the SQL Server engine use synchronous logical replication to achieve the same result, employing SQL Server-native Mirroring 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 Multi-AZ deployments also extend to planned maintenance and backups. In the case of system upgrades like OS patching or DB Instance scaling, these operations are applied first on the standby, prior to the automatic failover. As a result, your availability impact is, again, only the time required for automatic failover to complete.
Unlike Single-AZ deployments, I/O activity is not suspended on your primary during backup for Multi-AZ deployments for the MySQL, 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 Multi-AZ deployments.
On instance failure in Amazon Aurora deployments, Amazon RDS uses RDS Multi-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 connectivity 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.

QUESTION 88
Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS.

Which service should you use?

A. Amazon RDS with provisioned IOPS up to the anticipated peak write throughput.
B. Amazon Simple Queue Service (SQS) for capturing the writes and draining the queue to write to the database.

C. Amazon ElastiCache to store the writes until the writes are committed to the database.
D. Amazon DynamoDB with provisioned write throughput up to the anticipated peak write throughput.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. By using Amazon SQS, developers can simply move data between distributed application components performing different tasks, without losing messages or requiring each component to be always available. Amazon SQS makes it easy to build a distributed, decoupled application, working in close conjunction with the Amazon Elastic Compute Cloud (Amazon EC2) and the other AWS infrastructure web services. What can I do with Amazon SQS?
Amazon SQS is a web service that gives you access to a message queue that can be used to store messages while waiting for a computer to process them. This allows you to quickly build message queuing applications that can be run on any computer on the internet. Since Amazon SQS is highly scalable and you only pay for what you use, you can start small and grow your application as you wish, with no compromise on performance or reliability. This lets you focus on building sophisticated message-based applications, without worrying about how the messages are stored and managed. You can use Amazon SQS with software applications in various ways. For example, you can:
Integrate Amazon SQS with other AWS infrastructure web services to make applications more reliable and flexible.
Use Amazon SQS to create a queue of work where each message is a task that needs to be completed by a process. One or many computers can read tasks from the queue and perform them.
Build a microservices architecture, using queues to connect your microservices.
Keep notifications of significant events in a business process in an Amazon SQS queue. Each event can have a corresponding message in a queue, and applications that need to be aware of the event can read and process the messages.

QUESTION 89
You need a persistent and durable storage to trace call activity of an IVR (Interactive Voice Response) system. Call duration is mostly in the 2-3 minutes timeframe. Each traced call can be either active or terminated. An external application needs to know each minute the list of currently active calls. Usually there are a few calls/second, but once per month there is a periodic peak up to 1000 calls/second for a few hours. The system is open 24/7 and any downtime should be avoided. Historical data is periodically archived to files. Cost saving is a priority for this project.

What database implementation would better fit this scenario, keeping costs as low as possible?

A. Use DynamoDB with a "Calls" table and a Global Secondary Index on a "State" attribute that can equal to "active" or "terminated". In this way the Global Secondary Index can be used for all items in the table.
B. Use RDS Multi-AZ with a "CALLS" table and an indexed "STATE" field that can be equal to "ACTIVE" or 'TERMINATED". In this way the SQL query is optimized by the use of the Index.
C. Use RDS Multi-AZ with two tables, one for "ACTIVE_CALLS" and one for "TERMINATED_CALLS". In this way the "ACTIVE_CALLS" table is always small and effective to access.
D. Use DynamoDB with a "Calls" table and a Global Secondary Index on a "IsActive" attribute that is present for active calls only. In this way the Global Secondary Index is sparse and more effective.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Q: Can a global secondary index key be defined on non-unique attributes?
Yes. Unlike the primary key on a table, a GSI index does not require the indexed attributes to be unique. Q:
Are GSI key attributes required in all items of a DynamoDB table?
No. GSIs are sparse indexes. Unlike the requirement of having a primary key, an item in a DynamoDB table does not have to contain any of the GSI keys. If a GSI key has both hash and range elements, and a table item omits either of them, then that item will not be indexed by the corresponding GSI. In such cases, a GSI can be very useful in efficiently locating items that have an uncommon attribute.
Reference: https://aws.amazon.com/dynamodb/faqs/

QUESTION 90
Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design tor the application that leverages multiple regions tor the most recently accessed content and latency sensitive portions of the wet) site The most latency sensitive component of the application involves reading user preferences to support web site personalization and ad selection.

In addition to running your application in multiple regions, which option will support this application’s requirements?

A. Serve user content from S3. CloudFront and use Route53 latency-based routing between ELBs in each region Retrieve user preferences from a local DynamoDB table in each region and leverage SQS to capture changes to userpreferences with SOS workers for propagating updates to each table.
B. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3. CloudFront with dynamic content and an ELB in each region Retrieve user preferences from an ElasticCache cluster in eachregion and leverage SNS notifications to propagate user preference changes to a worker node in each region.
C. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3 CloudFront and Route53 latency-based routing Between ELBs In each region Retrieve user preferences from a DynamoDBtable and leverage SQS to capture changes to user preferences with SOS workers for propagating DynamoDB updates.

D. Serve user content from S3. CloudFront with dynamic content, and an ELB in each region Retrieve user preferences from an ElastiCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of userpreferences from a centralized OB to each ElastiCache cluster.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91 You've been brought in as solutions architect to assist an enterprise customer with their migration of an e-commerce platform to Amazon Virtual Private Cloud (VPC) The previous architect has already deployed a 3-tier VPC.

The configuration is as follows:
VPC: vpc-2f8bc447
IGW: igw-2d8bc445
NACL: ad-208bc448
Subnets and Route Tables:
Web servers: subnet-258bc44d
Application servers: subnet-248bc44c
Database servers: subnet-9189c6f9
Route Tables: rrb-218bc449 rtb-238bc44b Associations: subnet-258bc44d : rtb-218bc449 subnet-248bc44c : rtb-238bc44b subnet-9189c6f9 : rtb-238bc44b

You are now ready to begin deploying EC2 instances into the VPC Web servers must have direct access to the internet Application and database servers cannot have direct access to the internet.

Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?

A. Create a bastion and NAT instance in subnet-258bc44d, and add a route from rtb- 238bc44b to the NAT instance.
B. Add a route from rtb-238bc44b to igw-2d8bc445 and add a bastion and NAT instance within subnet-248bc44c.
C. Create a bastion and NAT instance in subnet-248bc44c, and add a route from rtb- 238bc44b to subnet-258bc44d.
D. Create a bastion and NAT instance in subnet-258bc44d, add a route from rtb-238bc44b to Igw-2d8bc445, and a new NACL that allows access between subnet-258bc44d and subnet-248bc44c.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
You are designing a multi-platform web application for AWS The application will run on EC2 instances and will be accessed from PCs. Tablets and smart phones Supported accessing platforms are Windows, MacOS, IOS and Android Separate sticky session and SSL certificate setups are required for different platform types.

Which of the following describes the most cost effective and performance efficient architecture setup?

A. Setup a hybrid architecture to handle session state and SSL certificates on-prem and separate EC2 Instance groups running web applications for different platform types running in a VPC.
B. Set up one ELB for all platforms to distribute load among multiple instance under it Each EC2 instance implements ail functionality for a particular platform.
C. Set up two ELBs The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.
D. Assign multiple ELBS to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type Session stickiness and SSL termination are done at the ELBs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
One ELB cannot handle different SSL certificates but since we are using sticky sessions it must be handled at the ELB level. SSL could be handled on the EC2 instances only with TCP configured ELB, ELB supports sticky sessions only in HTTP/HTTPS configurations.
The way the Elastic Load Balancer does session stickiness is on a HTTP/HTTPS listener is by utilizing an HTTP cookie. If SSL traffic is not terminated on the Elastic Load Balancer and is terminated on the back-end instance, the Elastic Load Balancer has no visibility into the HTTP headers and therefore can not set or read any of the HTTP headers being passed back and forth.
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html

QUESTION 93
An administrator is using Amazon CloudFormation to deploy a three tier web application that consists of a web tier and application tier that will utilize Amazon DynamoDB for storage when creating the CloudFormation template.

Which of the following would allow the application instance access to the DynamoDB tables without exposing API credentials?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Your company has recently extended its datacenter into a VPC on AWS to add burst computing capacity as needed Members of your Network Operations Center need to be able to go to the AWS Management Console and administer Amazon EC2 instances as necessary. You don't want to create new IAM users for each NOC member and make those users sign in again to the AWS Management Console.

Which option below will meet the needs for your NOC members?

A. Use OAuth 2.0 to retrieve temporary AWS security credentials to enable your NOC members to sign in to the AWS Management Console.
B. Use web Identity Federation to retrieve AWS temporary security credentials to enable your NOC members to sign in to the AWS Management Console.
C. Use your on-premises SAML 2.0-compliant identity provider (IDP) to grant the NOC members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint.
D. Use your on-premises SAML2.0-compliam identity provider (IDP) to retrieve temporary security credentials to enable NOC members to sign in to the AWS Management Console.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95 You have an application running on an EC2 Instance which will allow users to download flies from a private S3 bucket using a pre-signed URL. Before generating the URL the application should verify the existence of the file in S3.

How should the application use AWS credentials to access the S3 bucket securely?

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

user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload tor the new fiscal year benefit enrollment period plus some extra overhead Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a country where the benefits company has no customers. The web tier instances are so overloaded that benefit enrollment administrators cannot even SSH into them.

Which activity would be useful in defending against this attack?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Use AWS Identity and Access Management (IAM) to control who in your organization has permission to create and manage security groups and network ACLs (NACL). Isolate the responsibilities and roles for better defense. For example, you can give only your network administrators or security admin the permission to manage the security groups and restrict other roles.

QUESTION 97
You are developing a new mobile application and are considering storing user preferences in AWS.2w This would provide a more uniform cross-device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size Additionally 5 million customers are expected to use the application on a regular basis.

The solution needs to be cost-effective, highly available, scalable and secure, how would you design a solution to meet the above requirements?

A. Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials
B. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS. Web IdentityFederation, and DynamoDB Fine Grained Access Control to authenticate and authorize access.
C. Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data .The mobile application will query the user preferences from the read replicas. Leverage the MySQL user managementand access privilege system to manage security and access credentials.
D. Store the user preference data in S3 Setup a DynamoDB table with an item for each user and an item attribute pointing to the user' S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3object directly utilize STS, Web identity Federation, and S3 ACLs to authenticate and authorize access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
You deployed your company website using Elastic Beanstalk and you enabled log file rotation to S3. An Elastic Map Reduce job is periodically analyzing the logs on S3 to build a usage dashboard that you share with your CIO.
You recently improved overall performance of the website using Cloud Front for dynamic content delivery and your website as the origin. After this architectural change, the usage dashboard shows that the traffic on your website dropped by an order of magnitude.

How do you fix your usage dashboard?

A. Enable Cloud Front to deliver access logs to S3 and use them as input of the Elastic Map Reduce job.
B. Turn on Cloud Trail and use trail log tiles on S3 as input of the Elastic Map Reduce job
C. Change your log collection process to use Cloud Watch ELB metrics as input of the Elastic Map Reduce job
D. Use Elastic Beanstalk "Rebuild Environment" option to update log delivery to the Elastic Map Reduce job.
E. Use Elastic Beanstalk "Restart App server(s)" option to update log delivery to the Elastic Map Reduce job.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

QUESTION 99
A web-startup runs its very successful social news application on Amazon EC2 with an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application-servers, and DynamoDB as data store. The main web-application best runs on m2 x large instances since it is highly memory- bound Each new deployment requires semi-automated creation and testing of a new AMI for the application servers which takes quite a while ana is therefore only done once per week. Recently, a new chat feature has been implemented in nodejs and wails to be integrated in the architecture. First tests show that the new component is CPU bound Because the company has some experience with using Chef, they decided to streamline the deployment process and use AWS Ops Works as an application life cycle tool to simplify management of the application and reduce the deployment cycles.

What configuration in AWS Ops Works is necessary to integrate the new chat module in the most cost-efficient and flexible way?

A. Create one AWS OpsWorks stack, create one AWS Ops Works layer, create one custom recipe
B. Create one AWS OpsWorks stack create two AWS Ops Works layers, create one custom recipe
C. Create two AWS OpsWorks stacks create two AWS Ops Works layers, create one custom recipe D. Create two AWS OpsWorks stacks create two AWS Ops Works layers, create two custom recipe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100 Select the correct set of options. These are the initial settings for the default security group:

A. Allow no inbound traffic, Allow all outbound traffic and Allow instances associated with this security group to talk to each other
B. Allow all inbound traffic, Allow no outbound traffic and Allow instances associated with this security group to talk to each other
C. Allow no inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other
D. Allow all inbound traffic, Allow all outbound traffic and Does NOT allow instances associated with this security group to talk to each other

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
How can an EBS volume that is currently attached to an EC2 instance be migrated from one Availability Zone to another?

A. Detach the volume and attach it to another EC2 instance in the other AZ.
B. Simply create a new volume in the other AZ and specify the original volume as the source.
C. Create a snapshot of the volume, and create a new volume from the snapshot in the other AZ.
D. Detach the volume, then use the ec2-migrate-volume command to move it to another AZ.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
After launching an instance that you intend to serve as a NAT (Network Address Translation) device in a public subnet you modify your route tables to have the NAT device be the target of internet bound traffic of your private subnet. When you try and make an outbound connection to the internet from an instance in the private subnet, you are not successful.

Which of the following steps could resolve the issue?

A. Disabling the Source/Destination Check attribute on the NAT instance
B. Attaching an Elastic IP address to the instance in the private subnet
C. Attaching a second Elastic Network Interface (ENI) to the NAT instance, and placing it in the private subnet
D. Attaching a second Elastic Network Interface (ENI) to the instance in the private subnet, and placing it in the public subnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
http://docs.aws.amazon.com/workspaces/latest/adminguide/gsg_create_vpc.html
QUESTION 103
Your application provides data transformation services. Files containing data to be transformed are first uploaded to Amazon S3 and then transformed by a fleet of spot EC2 instances. Files submitted by your premium customers must be transformed with the highest priority.

How should you implement such a system?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104 Which of the following are characteristics of Amazon VPC subnets? (Choose 2)

A. Each subnet spans at least 2 Availability Zones to provide a high-availability environment.
B. Each subnet maps to a single Availability Zone.
C. CIDR block mask of /25 is the smallest range supported.
D. By default, all subnets can route between each other, whether they are private or public.
E. Instances in a private subnet can communicate with the Internet only if they have an Elastic IP.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105 In AWS, which security aspects are the customer's responsibility? (Choose 4)

A. Security Group and ACL (Access Control List) settings
B. Decommissioning storage devices
C. Patch management on the EC2 instance's operating system
D. Life-cycle management of IAM credentials
E. Controlling physical access to compute resources

F. Encryption of EBS (Elastic Block Storage) volumes

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

QUESTION 106 When you put objects in Amazon S3, what is the indication that an object was successfully stored?

A. A HTTP 200 result code and MD5 checksum, taken together, indicate that the operation was successful.
B. Amazon S3 is engineered for 99.999999999% durability. Therefore there is no need to confirm that data was inserted.
C. A success code is inserted into the S3 object metadata.
D. Each S3 account has a special bucket named _s3_logs. Success codes are written to this bucket with a timestamp and checksum.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107 Within the IAM service a GROUP is regarded as a:

A. A collection of AWS accounts
B. It's the group of EC2 machines that gain the permissions specified in the GROUP.
C. There's no GROUP in IAM, but only USERS and RESOURCES.
D. A collection of users.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Use groups to assign permissions to IAM users
Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.), define the relevant permissions for each group, and then assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. That way, you can make changes for everyone in a group in just one place. As people move around in your company, you can simply change what IAM group their IAM user belongs to. http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions

QUESTION 108
Amazon EC2 provides a repository of public data sets that can be seamlessly integrated into AWS cloud-based applications.

What is the monthly charge for using the public data sets?

A. A 1-time charge of 10$ for all the datasets.
B. 1$ per dataset per month
C. 10$ per month for all the datasets
D. There is no charge for using the public data sets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
In the Amazon RDS Oracle DB engine, the Database Diagnostic Pack and the Database Tuning Pack are only available with __________.

A. Oracle Standard Edition
B. Oracle Express Edition
C. Oracle Enterprise Edition
D. None of these

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.pythian.com/blog/a-most-simple-cloud-is-amazon-rds-for-oracle-right-for-you/

QUESTION 110
A 3-Ber e-commerce web application is currently deployed on-premises, and will be migrated to AWS for greater scalability and elasticity. The web tier currently shares read-only data using a network distributed file system. The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast. The database tier uses shared-storage clustering to provide database failover capability, and uses several read slaves for scaling. Data on all servers and the distributed file system directory is backed up weekly to off-site tapes.

Which AWS storage and database architecture meets the requirements of the application?

A. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast.Database: use RDS with multi-AZ deployment and one or more read replicas.
Backup: web servers, app servers, and database backed up weekly to Glacier using snapshots.
B. Web servers: store read-only data in an EC2 NFS server, mount to each web server at boot time. App servers: share state using a combination of DynamoDB and IP multicast.
Database: use RDS with multi- AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots. C.
Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers:
share state using a combination of DynamoDB and IP unicast.
Database: use RDS with multi-AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
D. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time App
servers:
share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment.
Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Glacier doesn't suit all storage situations. Listed following are a few storage needs for which you should consider other AWS storage options instead of Amazon Glacier.
Data that must be updated very frequently might be better served by a storage solution with lower read/write latencies, such as Amazon EBS, Amazon RDS, Amazon DynamoDB, or relational databases running on EC2.
https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf

QUESTION 111
A user is running a batch process on EBS backed EC2 instances. The batch process launches few EC2 instances to process Hadoop Map reduce jobs which can run between 50 ?600 minutes or sometimes for even more time. The user wants a configuration that can terminate the instance only when the process is completed.

How can the user configure this with CloudWatch?

A. Configure a job which terminates all instances after 600 minutes
B. It is not possible to terminate instances automatically
C. Configure the CloudWatch action to terminate the instance when the CPU utilization falls below 5%D. Set up the CloudWatch with Auto Scaling to terminate all the instances

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which terminates the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

QUESTION 112
What is the maximum write throughput I can provision for a single Dynamic DB table?

A. 1,000 write capacity units
B. 100,000 write capacity units
C. Dynamic DB is designed to scale without limits, but if you go beyond 10,000 you have to contact AWS first.D. 10,000 write capacity units

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/dynamodb/faqs/

QUESTION 113
What is the name of licensing model in which I can use your existing Oracle Database licenses to run Oracle deployments on Amazon RDS?

A. Bring Your Own License
B. Role Bases License
C. Enterprise License
D. License Included

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://aws.amazon.com/oracle/

QUESTION 114 When you resize the Amazon RDS DB instance, Amazon RDS will perform the upgrade during the next maintenance window. If you want the upgrade to be performed now, rather than waiting for the maintenance window, specify the option.

A. ApplyNow
B. ApplySoon
C. ApplyThis
D. ApplyImmediately

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html

QUESTION 115 If I write the below command,
what does it do?

```
ec2-run ami-e3a5408a -n 20 -g appserver
```

A. Start twenty instances as members of appserver group.
B. Creates 20 rules in the security group named appserverC. Terminate twenty instances as members of appserver group.
D. Start 20 security groups

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
The ________ service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console.

A. Amazon RDS
B. AWS Integrity Management
C. AWS Identity and Access Management
D. Amazon EMR

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: https://aws.amazon.com/documentation/iam/?nc1=h_ls

QUESTION 117
Which AWS instance address has the following characteristics? :"If you stop an instance, its Elastic IP address is unmapped, and you must remap it when you restart the instance."

A. Both A and B
B. None of these
C. VPC Addresses
D. EC2 Addresses

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Stopping an instance EC2-
Classic
If you stop an instance, its Elastic IP address is disassociated, and you must reassociate the Elastic IP address when you restart the instance.
EC2-VPC If you stop an instance, its Elastic IP address remains
associated.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

QUESTION 118
By default, Amazon Cognito maintains the last-written version of the data. You can override this behavior and resolve data conflicts programmatically.
In addition, push synchronization allows you to use Amazon Cognito to send a silent notification to all devices associated with an identity to notify them that new data is available.

A. get

B. post
C. pull
D. push

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
http://aws.amazon.com/cognito/faqs/

QUESTION 119
You want to use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC).

What criterion must be met for this to be possible?

A. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access only the public AWS CodeDeploy endpoint.
B. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access only the public Amazon S3 service endpoint.
C. The AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access the public AWS CodeDeploy and Amazon S3 service endpoints.
D. It is not currently possible to use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC.)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use AWS CodeDeploy to deploy an application to Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC).
However, the AWS CodeDeploy agent installed on the Amazon EC2 instances must be able to access the public AWS CodeDeploy and Amazon S3 service endpoints. http://aws.amazon.com/codedeploy/faqs/

QUESTION 120
An IAM user is trying to perform an action on an object belonging to some other root account's bucket.

Which of the below mentioned options will AWS S3 not verify?

A. The object owner has provided access to the IAM user
B. Permission provided by the parent of the IAM user on the bucket
C. Permission provided by the bucket owner to the IAM user
D. Permission provided by the parent of the IAM user

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the IAM user is trying to perform some action on the object belonging to another AWS user's bucket, S3 will verify whether the owner of the IAM user has given sufficient permission to him. It also verifies the policy for the bucket as well as the policy defined by the object owner. http://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-auth-workflow-object-operation.html

QUESTION 121
An organization is planning to extend their data center by connecting their DC with the AWS VPC using the VPN gateway. The organization is setting up a dynamically routed VPN connection.

Which of the below mentioned answers is not required to setup this configuration?

A. The type of customer gateway, such as Cisco ASA, Juniper J-Series, Juniper SSG, Yamaha.
B. Elastic IP ranges that the organization wants to advertise over the VPN connection to the VPC.

C. Internet-routable IP address (static) of the customer gateway's external interface.

D. Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. The organization wants to extend their network into the cloud and also directly access the internet from their AWS VPC. Thus, the organization should setup a Virtual Private Cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with their data center network over an IPsec VPN tunnel. To setup this configuration the organization needs to use the Amazon VPC with a VPN connection. The organization network administrator must designate a physical appliance as a customer gateway and configure it. The organization would need the below mentioned information to setup this configuration:
The type of customer gateway, such as Cisco ASA, Juniper J-Series, Juniper SSG, Yamaha Internet-routable IP address (static) of the customer gateway's external interface Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the customer gateway, if the organization is creating a dynamically routed VPN connection. Internal network IP ranges that the user wants to advertise over the VPN connection to the VPC.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

QUESTION 122 In the context of AWS IAM, identify a true statement about user passwords (login profiles).

A. They must contain Unicode characters.

B. They can contain any Basic Latin (ASCII) characters.

C. They must begin and end with a forward slash (/).

D. They cannot contain Basic Latin (ASCII) characters.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user passwords (login profiles) of IAM users can contain any Basic Latin (ASCII)characters. http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

QUESTION 123
An organization is planning to host a Wordpress blog as well a joomla CMS on a single instance launched with VPC. The organization wants to have separate domains for each application and assign them using Route 53. The organization may have about ten instances each with two applications as mentioned above. While launching the instance, the organization configured two separate network interfaces (primary + ENI) and wanted to have two elastic IPs for that instance. It was suggested to use a public IP from AWS instead of an elastic IP as the number of elastic IPs is restricted.

What action will you recommend to the organization?

A. I agree with the suggestion but will prefer that the organization should use separate subnets with each ENI for different public IPs.

B. I do not agree as it is required to have only an elastic IP since an instance has more than one ENI and AWS does not assign a public IP to an instance with multiple ENIs.

C. I do not agree as AWS VPC does not attach a public IP to an ENI; so the user has to use only an elastic IP only.

D. I agree with the suggestion and it is recommended to use a public IP from AWS since the organization is going to use DNS with Route 53.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. An Elastic Network Interface (ENI) is a virtual network interface that the user can attach to an instance in a VPC. The user can attach up to two ENIs with a single instance. However, AWS cannot assign a public IP when there are two ENIs attached to a single instance. It is recommended to assign an elastic IP in this scenario. If the organization wants more than 5 EIPs they can request AWS to increase the number. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 124 What is the default maximum number of VPCs allowed per region?

A. 5

B. 10
C. 100
D. 15

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The maximum number of VPCs allowed per region is 5.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html

QUESTION 125
A customer has a website which shows all the deals available across the market. The site experiences a load of 5 large EC2 instances generally.
However, a week before Thanksgiving vacation they encounter a load of almost 20 large instances. The load during that period varies over the day based on the office timings.

Which of the below mentioned solutions is cost effective as well as help the website achieve better performance?

A. Setup to run 10 instances during the pre-vacation period and only scale up during the office time by launching 10 more instances using the AutoScaling schedule.
B. Keep only 10 instances running and manually launch 10 instances every day during office hours.
C. During the pre-vacation period setup 20 instances to run continuously.
D. During the pre-vacation period setup a scenario where the organization has 15 instances running and 5 instances to scale up and down using Auto Scaling based on the network I/O policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS provides an on demand, scalable infrastructure. AWS EC2 allows the user to launch On- Demand instances and the organization should create an AMI of the running instance. When the organization is experiencing varying loads and the time of the load is not known but it is higher than the routine traffic it is recommended that the organization launches a few instances beforehand and then setups AutoScaling with policies which scale up and down as per the EC2 metrics, such as Network I/O or CPU utilization. If the organization keeps all 10 additional instances as a part of the AutoScaling policy sometimes during a sudden higher load it may take time to launch instances and may not give an optimal performance. This is the reason it is recommended that the organization keeps an additional 5 instances running and the next 5 instances scheduled as per the AutoScaling policy for cost effectiveness.

QUESTION 126
An organization is setting a website on the AWS VPC. The organization has blocked a few IPs to avoid a D-DOS attack.

How can the organization configure that a request from the above mentioned IPs does not access the application instances?

A. Create an IAM policy for VPC which has a condition to disallow traffic from that IP address.
B. Configure a security group at the subnet level which denies traffic from the selected IP.
C. Configure the security group with the EC2 instance which denies access from that IP address.
D. Configure an ACL at the subnet which denies the traffic from that IP address.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. AWS provides two features that the user can use to increase security in VPC: security groups and network ACLs. Security group works at the instance level while ACL works at the subnet level. ACL allows both allow and deny rules. Thus, when the user wants to reject traffic from the selected IPs it is recommended to use ACL with subnets.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

QUESTION 127

An organization has 4 people in the IT operations team who are responsible to manage the AWS infrastructure. The organization wants to setup that each user will have access to launch and manage an instance in a zone which the other user cannot modify.

Which of the below mentioned options is the best solution to set this up?

A. Create four AWS accounts and give each user access to a separate account.
B. Create an IAM user and allow them permission to launch an instance of a different sizes only.
C. Create four IAM users and four VPCs and allow each IAM user to have access to separate VPCs.
D. Create a VPC with four subnets and allow access to each subnet for the individual IAM user.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC. The VPC also work with IAM and the organization can create IAM users who have access to various VPC services. The organization can setup access for the IAM user who can modify the security groups of the VPC. The sample policy is given below:

```
{
"Version": "2012-10-17",
"Statement":
[{ "Effect": "Allow",
"Action": "ec2:RunInstances", "Resource":
["arn:aws:ec2:region::image/ami-*", "arn:aws:ec2:region:account:subnet/subnet-1a2b3c4d", "arn:aws:ec2:region:account:network-interface/*", "arn:aws:ec2:region:account:volume/*", "arn:aws:ec2:region:account:key-pair/*",
"arn:aws:ec2:region:account:security-group/sg-123abc123" ] }]
}
```

With this policy the user can create four subnets in separate zones and provide IAM user access to each subnet.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_IAM.html

QUESTION 128
An organization is planning to host an application on the AWS VPC. The organization wants dedicated instances. However, an AWS consultant advised the organization not to use dedicated instances with VPC as the design has a few limitations.

Which of the below mentioned statements is not a limitation of dedicated instances with VPC?

A. All instances launched with this VPC will always be dedicated instances and the user cannot use a default tenancy model for them.
B. It does not support the AWS RDS with a dedicated tenancy VPC.
C. The user cannot use Reserved Instances with a dedicated tenancy model.
D. The EBS volume will not be on the same tenant hardware as the EC2 instance though the user has configured dedicated tenancy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Dedicated instances are Amazon EC2 instances that run in a Virtual Private Cloud (VPC) on hardware that is dedicated to a single customer. The client's dedicated instances are physically isolated at the host hardware level from instances that are not dedicated instances as well as from instances that belong to other AWS accounts. All instances launched with the dedicated tenancy model of VPC will always be dedicated instances. Dedicated tenancy has a limitation that it may not support a few services, such as RDS. Even the EBS will not be on dedicated hardware. However, the user can save some cost as well as reserve some capacity by using a Reserved Instance model with dedicated tenancy. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html

QUESTION 129 In which step of using AWS Direct Connect should the user determine the required port speed?

A. Complete the Cross Connect
B. Verify Your Virtual Interface
C. Download Router Configuration

D. Submit AWS Direct Connect Connection Request

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To submit an AWS Direct Connect connection request, you need to provide the following information:
Your contact information.
The AWS Direct Connect Location to connect to.
Details of AWS Direct Connect partner if you use the AWS Partner Network (APN) service. The port speed you require, either 1 Gbps or 10 Gbps.
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#ConnectionRequest

QUESTION 130 In Amazon IAM, what is the maximum length
for a role name?

A. 128 characters
B. 512 characters
C. 64 characters
D. 256 characters

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon IAM, the maximum length for a role name is 64 characters.
http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

QUESTION 131
A user is planning to host a web server as well as an app server on a single EC2 instance which is a part of the public subnet of a VPC.

How can the user setup to have two separate public IPs and separate security groups for both the application as well as the web server?

A. Launch VPC with two separate subnets and make the instance a part of both the subnets.
B. Launch a VPC instance with two network interfaces. Assign a separate security group and elastic IP to them.
C. Launch a VPC instance with two network interfaces. Assign a separate security group to each and AWS will assign a separate public IP to them.
D. Launch a VPC with ELB such that it redirects requests to separate VPC instances of the public subnet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you need to host multiple websites (with different IPs) on a single EC2 instance, the following is the suggested method from AWS. Launch a VPC instance with two network interfaces.
Assign elastic IPs from VPC EIP pool to those interfaces (Because, when the user has attached more than one network interface with an instance, AWS cannot assign public IPs to them.) Assign separate Security Groups if separate Security Groups are needed This scenario also helps for operating network appliances, such as firewalls or load balancers that have multiple private IP addresses for each network interface.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html

QUESTION 132
You have subscribed to the AWS Business and Enterprise support plan.
Your business has a backlog of problems, and you need about 20 of your IAM users to open technical support cases.

How many users can open technical support cases under the AWS Business and Enterprise support plan?

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

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
In the context of AWS support, the Business and Enterprise support plans allow an unlimited number of users to open technical support cases (supported by AWS Identity and Access Management (IAM)).
https://aws.amazon.com/premiumsupport/faqs/

QUESTION 133 While implementing the policy keys in AWS Direct Connect, if you use and the request comes from an Amazon EC2 instance, the instance's public IP address is evaluated to determine if access is allowed.

A. aws:SecureTransport
B. aws:EpochIP
C. aws:SourceIp
D. aws:CurrentTime

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
While implementing the policy keys in Amazon RDS, if you use aws: SourceIp and the request comes from an Amazon EC2 instance, the instance's public IP address is evaluated to determine if access is allowed.
http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html

QUESTION 134
How many g2.2xlarge on-demand instances can a user run in one region without taking any limit increase approval from AWS?

A. 20
B. 2C. 5
D. 10

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Generally, AWS EC2 allows running 20 on-demand instances and 100 spot instances at a time. This limit can be increased by requesting at https://aws.amazon.com/contact-us/ec2-request. Excluding certain types of instances, the limit is lower than mentioned above. For g2.2xlarge, the user can run only 5 on-demand instance at a time. http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

QUESTION 135
A user has created a MySQL RDS instance with PIOPS. Which of the below mentioned statements will help user understand the advantage of PIOPS?

A. The user can achieve additional dedicated capacity for the EBS I/O with an enhanced RDS option
B. It uses a standard EBS volume with optimized configuration the stacks
C. It uses optimized EBS volumes and optimized configuration stacks
D. It provides a dedicated network bandwidth between EBS and RDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RDS DB instance storage comes in two types: standard and provisioned IOPS. Standard storage is allocated on the Amazon EBS volumes and connected to the user's DB instance. Provisioned IOPS uses optimized EBS volumes and an optimized configuration stack. It provides additional, dedicated capacity for the EBS I/O. http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

QUESTION 136
A user authenticating with Amazon Cognito will go through a multi-step process to bootstrap their credentials. Amazon Cognito has two different flows for authentication with public providers.

Which of the following are the two flows?

A. Authenticated and non-authenticated
B. Public and private
C. Enhanced and basic
D. Single step and multistep

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user authenticating with Amazon Cognito will go through a multi-step process to bootstrap their credentials. Amazon Cognito has two different flows for authentication with public providers: enhanced and basic.
http://docs.aws.amazon.com/cognito/devguide/identity/concepts/authentication-flow/

QUESTION 137 Which of the following is the Amazon Resource Name (ARN) condition operator that can be used within an Identity and Access Management (IAM) policy to check the case-insensitive matching of the ARN?

A. ArnCheck
B. ArnMatch
C. ArnCase
D. ArnLike

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Resource Name (ARN) condition operators let you construct Condition elements that restrict access based on comparing a key to an ARN. ArnLike, for instance, is a case-insensitive matching of the ARN. Each of the six colondelimited components of the ARN is checked separately and each can include a multi-character match wildcard (*) or a single-character match wildcard (?).
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

QUESTION 138
An organization is creating a VPC for their application hosting. The organization has created two private subnets in the same AZ and created one subnet in a separate zone. The organization wants to make a HA system with the internal ELB.

Which of these statements is true with respect to an internal ELB in this scenario?

A. ELB can support only one subnet in each availability zone.
B. ELB does not allow subnet selection; instead it will automatically select all the available subnets of the VPC.
C. If the user is creating an internal ELB, he should use only private subnets.
D. ELB can support all the subnets irrespective of their zones.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud.
The user has complete control over the virtual networking environment. Within this virtual private cloud, the user can launch AWS resources, such as an ELB, and EC2 instances.
There are two ELBs available with VPC: internet facing and internal (private) ELB. For internal servers, such as App servers the organization can create an internal load balancer in their VPC and then place back-end application instances behind the internal load balancer.
The internal load balancer will route requests to the back-end application instances, which are also using private IP addresses and only accept requests from the internal load balancer. The
Internal ELB supports only one subnet in each AZ and asks the user to select a subnet while configuring internal ELB.
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/USVPC_creating_basic_lb.html

QUESTION 139
In Amazon ElastiCache, the failure of a single cache node can have an impact on the availability of your application and the load on your back-end database while ElastiCache provisions a replacement for the failed cache node and it get repopulated.

Which of the following is a solution to reduce this potential availability impact?

A. Spread your memory and compute capacity over fewer number of cache nodes, each with smaller capacity.
B. Spread your memory and compute capacity over a larger number of cache nodes, each with smaller capacity.
C. Include fewer number of high capacity nodes.
D. Include a larger number of cache nodes, each with high capacity.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon ElastiCache, the number of cache nodes in the cluster is a key factor in the availability of your cluster running Memcached. The failure of a single cache node can have an impact on the availability of your application and the load on your back-end database while ElastiCache provisions a replacement for the failed cache node and it get repopulated.
You can reduce this potential availability impact by spreading your memory and compute capacity over a larger number of cache nodes, each with smaller capacity, rather than using a fewer number of high capacity nodes.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/CacheNode.Memcached.html

QUESTION 140
MapMySite is setting up a web application in the AWS VPC. The organization has decided to use an AWS RDS instead of using its own DB instance for HA and DR requirements. The
organization also wants to secure RDS access.

How should the web application be setup with RDS?

A. Create a VPC with one public and one private subnet. Launch an application instance in the public subnet while RDS is launched in the private subnet.
B. Setup a public and two private subnets in different AZs within a VPC and create a subnet group. Launch RDS with that subnet group.
C. Create a network interface and attach two subnets to it. Attach that network interface with RDS while launching a DB instance.
D. Create two separate VPCs and launch a Web app in one VPC and RDS in a separate VPC and connect them with VPC peering.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources, such as RDS into a virtual network that the user has defined. Subnets are segments of a VPC's IP address range that the user can designate to a group of VPC resources based on the security and operational needs.
A DB subnet group is a collection of subnets (generally private) that a user can create in a VPC and assign to the RDS DB instances. A DB subnet group allows the user to specify a particular VPC when creating the DB instances. Each DB subnet group should have subnets in at least two Availability Zones in a given region. http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.html

QUESTION 141
When does an AWS Data Pipeline terminate the AWS Data Pipeline-managed compute resources?

A. AWS Data Pipeline terminates AWS Data Pipeline-managed compute resources every 2 hours.

B. When the final activity that uses the resources is running

C. AWS Data Pipeline terminates AWS Data Pipeline-managed compute resources every 12 hours.D. When the final activity that uses the resources has completed successfully or failed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Compute resources will be provisioned by AWS Data Pipeline when the first activity for a scheduled time that uses those resources is ready to run, and those instances will be terminated when the final activity that uses the resources has completed successfully or failed. https://aws.amazon.com/datapipeline/faqs/

QUESTION 142 What bandwidths do AWS Direct Connect currently support?

A. 10Mbps and 100Mbps

B. 10Gbps and 100Gbps

C. 100Mbps and 1Gbps

D. 1Gbps and 10 Gbps

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connection currently supports 1Gbps and 10 Gbps.
http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION 143 The Principal element of an IAM policy refers to the specific entity that should be allowed or denied permission, whereas the translates to everyone except the specified entity.

A. NotPrincipal

B. Vendor

C. Principal

D. Action

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The element NotPrincipal that is included within your IAM policy statements allows you to specify an exception to a list of principals to whom the access to a specific resource is either allowed or denied. Use the NotPrincipal element to specify an exception to a list of principals. For example, you can deny access to all principals except the one named in the NotPrincipal element. http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html#Principal

QUESTION 144
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 address IP 10.201.31.6 is currently assigned to another interface

B. Private IP address 10.201.31.6 is reserved by Amazon for IP networking purposes.

C. Private IP address 10.201.31.6 is blocked via ACLs in Amazon infrastructure as a part of platform security.

D. Private IP address 10.201.31.6 is not part of the associated subnet's IP address range.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
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 http://aws.amazon.com/vpc/faqs/

QUESTION 145 A user is configuring MySQL RDS with PIOPS. What should be the minimum size of DB storage provided by the user?

A. 1 TB
B. 50 GB
C. 5 GB
D. 100 GB

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the user is trying to enable PIOPS with MySQL RDS, the minimum size of storage should be 100 GB.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.html

QUESTION 146
The Statement element, of an AWS IAM policy, contains an array of individual statements. Each individual statement is a(n) _________ block enclosed in braces { }.

A. XML
B. JavaScript
C. JSON
D. AJAX

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Statement element, of an IAM policy, contains an array of individual statements. Each individual statement is a JSON block enclosed in braces { }.
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

QUESTION 147
If no explicit deny is found while applying IAM's Policy Evaluation Logic, the enforcement code looks for any ______ instructions that would apply to the request.

A. "cancel"
B. "suspend"
C. "allow”
D. "valid"

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If an explicit deny is not found among the applicable policies for a specific request, IAM's Policy Evaluation Logic checks for any "allow" instructions to check if the request can be successfully completed.
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

QUESTION 148
An organization is hosting a scalable web application using AWS. The organization has configured ELB and Auto Scaling to make the application scalable.
Which of the below mentioned statements is not required to be followed for ELB when the application is planning to host a web application on VPC?

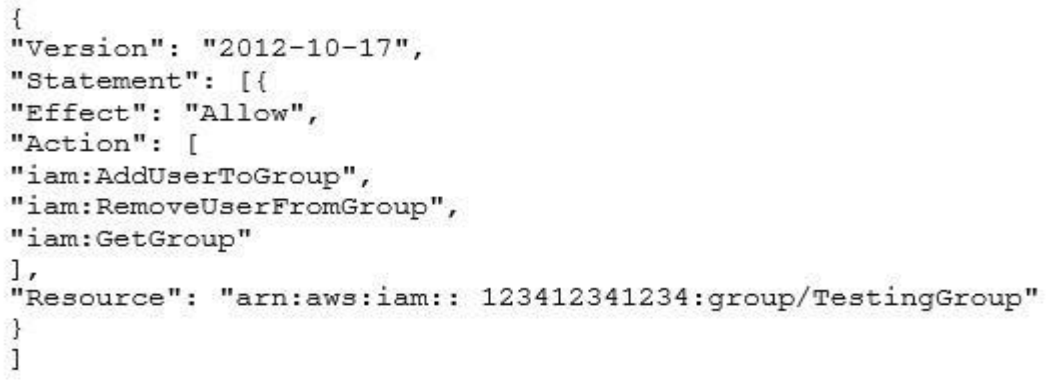
A. The ELB and all the instances should be in the same subnet.
B. Configure the security group rules and network ACLs to allow traffic to be routed between the subnets in the VPC.
C. The internet facing ELB should have a route table associated with the internet gateway.
D. The internet facing ELB should be only in a public subnet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Within this virtual private cloud, the user can launch AWS resources, such as an ELB, and EC2 instances. There are two ELBs available with VPC: internet facing and internal (private) ELB. For the internet facing ELB it is required that the ELB should be in a public subnet. After the user creates the public subnet, he should ensure to associate the route table of the public subnet with the internet gateway to enable the load balancer in the subnet to connect with the internet. The ELB and instances can be in a separate subnet. However, to allow communication between the instance and the ELB the user must configure the security group rules and network ACLs to allow traffic to be routed between the subnets in his VPC. http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/CreateVPCForELB.html

QUESTION 149
An organization (account ID 123412341234) has configured the IAM policy to allow the user to modify his credentials.

What will the below mentioned statement allow the user to perform?



```
{
"Version": "2012-10-17",
"Statement": [{
"Effect": "Allow",
"Action": [
"iam:AddUserToGroup",
"iam:RemoveUserFromGroup",
"iam:GetGroup"
],
"Resource": "arn:aws:iam:: 123412341234:group/TestingGroup"
}
]
```

A. Allow the IAM user to update the membership of the group called TestingGroup
B. The IAM policy will throw an error due to an invalid resource name
C. The IAM policy will allow the user to subscribe to any IAM group
D. Allow the IAM user to delete the TestingGroup

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the organization (account ID 123412341234) wants their users to manage their subscription to the groups, they should create a relevant policy for that. The below mentioned policy allows the respective IAM user to update the membership of the group called MarketingGroup.
{
"Version": "2012-10-17",
"Statement": [{
"Effect": "Allow", "Action": ["iam:AddUserToGroup",
"iam:RemoveUserFromGroup", "iam:GetGroup"

],
"Resource": "arn:aws:iam:: 123412341234:group/ TestingGroup " }]
http://docs.aws.amazon.com/IAM/latest/UserGuide/Credentials-Permissions-examples.html#creds-policies-credentials

QUESTION 150 A user has configured EBS volume with PIOPS. The user is not experiencing the optimal throughput.

Which of the following could not be factor affecting I/O performance of that EBS volume?

A. EBS bandwidth of dedicated instance exceeding the PIOPS
B. EBS volume size
C. EC2 bandwidth
D. Instance type is not EBS optimized

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the user is not experiencing the expected IOPS or throughput that is provisioned, ensure that the EC2 bandwidth is not the limiting factor, the instance is EBS-optimized (or include 10 Gigabit network connectivity) and the instance type EBS dedicated bandwidth exceeds the IOPS more than he has provisioned. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html

QUESTION 151 How can multiple compute resources be used on the same pipeline in AWS Data Pipeline?

A. You can use multiple compute resources on the same pipeline by defining multiple cluster objects in your definition file and associating the cluster to use for each activity via its runs On field.
B. You can use multiple compute resources on the same pipeline by defining multiple cluster definition filesC. You can use multiple compute resources on the same pipeline by defining multiple clusters for your activity.
D. You cannot use multiple compute resources on the same pipeline.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Multiple compute resources can be used on the same pipeline in AWS Data Pipeline by defining multiple cluster objects in your definition file and associating the cluster to use for each activity via its runs On field, which allows pipelines to combine AWS and on premise resources, or to use a mix of instance types for their activities. https://aws.amazon.com/datapipeline/faqs/

QUESTION 152 The two policies that you attach to an IAM role are the access policy and the trust policy. The trust policy identifies who can assume the role and grants the permission in the AWS Lambda account principal by adding the _______ action.

A. aws:AssumeAdmin
B. lambda:InvokeAsync
C. sts:InvokeAsyncD. sts:AssumeRole

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The two policies that you attach to an IAM role are the access policy and the trust policy. Remember that adding an account to the trust policy of a role is only half of establishing the trust relationship. By default, no users in the trusted accounts can assume the role until the administrator for that account grants the users the permission to assume the role by adding the Amazon Resource Name (ARN) of the role to an Allow element for the sts:AssumeRole action.
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_manage_modify.html

QUESTION 153
The MySecureData company has five branches across the globe. They want to expand their data centers such that their web server will be in the AWS and each branch would have their own database in the local data center. Based on the user login, the company wants to connect to the data center.
How can MySecureData company implement this scenario with the AWS VPC?

A. Create five VPCs with the public subnet for the app server and setup the VPN gateway for each VPN to connect them individually.
B. Use the AWS VPN CloudHub to communicate with multiple VPN connections.
C. Use the AWS CloudGateway to communicate with multiple VPN connections.
D. It is not possible to connect different data centers from a single VPC.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. If the organization has multiple VPN connections, he can provide secure communication between sites using the AWS VPN CloudHub.
The VPN CloudHub operates on a simple hub-and-spoke model that the user 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 connectivity between remote offices. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

QUESTION 154
One of your AWS Data Pipeline activities has failed consequently and has entered a hard failure state after retrying thrice.

You want to try it again. Is it possible to increase the number of automatic retries to more than thrice?

A. Yes, you can increase the number of automatic retries to 6.
B. Yes, you can increase the number of automatic retries to indefinite number.
C. No, you cannot increase the number of automatic retries.
D. Yes, you can increase the number of automatic retries to 10.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS Data Pipeline, an activity fails if all of its activity attempts return with a failed state. By default, an activity retries three times before entering a hard failure state. You can increase the number of automatic retries to 10. However, the system does not allow indefinite retries. https://aws.amazon.com/datapipeline/faqs/

QUESTION 155 True or False: In Amazon ElastiCache replication groups of Redis, for performance tuning reasons, you can change the roles of the cache nodes within the replication group, with the primary and one of the replicas exchanging roles.

A. True, however, you get lower performance.
B. FALSE
C. TRUE
D. False, you must recreate the replication group to improve performance tuning.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon ElastiCache, a replication group is a collection of Redis Cache Clusters, with one primary read-write cluster and up to five secondary, read-only clusters, which are called read replicas. You can change the roles of the cache clusters within the replication group, with the primary cluster and one of the replicas exchanging roles. You might decide to do this for performance tuning reasons.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/Replication.Redis.Groups.html

QUESTION 156 How much memory does the cr1.8xlarge instance type provide?

A. 224 GB
B. 124 GB
C. 184 GB
D. 244 GB

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The CR1 instances are part of the memory optimized instances. They offer lowest cost per GB RAM among all the AWS instance families. CR1 instances are part of the new generation of memory optimized instances, which can offer up to 244 GB RAM and run on faster CPUs (Intel Xeon E5-2670 with NUMA support) in comparison to the M2 instances of the same family. They support cluster networking for bandwidth intensive applications. cr1.8xlarge is one of the largest instance types of the CR1 family, which can offer 244 GB RAM. http://aws.amazon.com/ec2/instance-types/

QUESTION 157
How many cg1.4xlarge on-demand instances can a user run in one region without taking any limit increase approval from AWS?

A. 20
B. 2C. 5
D. 10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Generally, AWS EC2 allows running 20 on-demand instances and 100 spot instances at a time. This limit can be increased by requesting at https://aws.amazon.com/contact-us/ec2-request. Excluding certain types of instances, the limit is lower than mentioned above. For cg1.4xlarge, the user can run only 2 on-demand instances at a time.
http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

QUESTION 158
Regarding Amazon SNS, you can send notification messages to mobile devices through any of the following supported push notification services, EXCEPT:

A. Microsoft Windows Mobile Messaging (MWMM)
B. Google Cloud Messaging for Android (GCM)
C. Amazon Device Messaging (ADM)
D. Apple Push Notification Service (APNS)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon SNS, you have the ability to send notification messages directly to apps on mobile devices. Notification messages sent to a mobile endpoint can appear in the mobile app as message alerts, badge updates, or even sound alerts. Microsoft Windows Mobile Messaging (MWMM) doesn't exist and is not supported by Amazon SNS. http://docs.aws.amazon.com/sns/latest/dg/SNSMobilePush.html

QUESTION 159
You want to define permissions for a role in an IAM policy. Which of the following configuration formats should you use?
A. An XML document written in the IAM Policy Language
B. An XML document written in a language of your choice
C. A JSON document written in the IAM Policy Language
D. JSON document written in a language of your choice

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You define the permissions for a role in an IAM policy. An IAM policy is a JSON document written in the IAM Policy Language. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html

QUESTION 160
IAM Secure and Scalable is an organization which provides scalable and secure SAAS to its clients. They are planning to host a web server and App server on AWS VPC as separate tiers. The organization wants to implement the scalability by configuring Auto Scaling and load balancer with their app servers (middle tier) too.

Which of the below mentioned options suits their requirements?

A. Since ELB is internet facing, it is recommended to setup HAProxy as the Load balancer within the VPC.
B. Create an Internet facing ELB with VPC and configure all the App servers with it.
C. The user should make ELB with EC2-CLASSIC and enable SSH with it for security.
D. Create an Internal Load balancer with VPC and register all the App servers with it.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Within this virtual private cloud, the user can launch AWS resources, such as an ELB, and EC2 instances.
There are two ELBs available with VPC: internet facing and internal (private) ELB. For internal servers, such as App servers the organization can create an internal load balancer in their VPC and then place back-end application instances behind the internal load balancer. The internal load balancer will route requests to the back-end application instances, which are also using private IP addresses and only accept requests from the internal load balancer.

Reference: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/vpc-loadbalancer-types.html

QUESTION 161 True or False: Amazon ElastiCache supports the Redis
key-value store.

A. True, ElastiCache supports the Redis key-value store, but with limited functionalities.
B. False, ElastiCache does not support the Redis key-value store.
C. True, ElastiCache supports the Redis key-value store.
D. False, ElastiCache supports the Redis key-value store only if you are in a VPC environment.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is true. ElastiCache supports two open-source in-memory caching engines: 1. Memcached - a widely adopted memory object caching system. ElastiCache is protocol compliant with Memcached, so popular tools that you use today with existing Memcached environments will work seamlessly with the service. 2. Redis - a popular open-source in-memory key-value store that supports data structures such as sorted sets and lists. ElastiCache supports Master / Slave replication and Multi-AZ which can be used to achieve cross AZ redundancy. Reference: https://aws.amazon.com/elasticache/

QUESTION 162
Which of the following is NOT an advantage of using AWS Direct Connect?

A. AWS Direct Connect provides users access to public and private resources by using two different connections while maintaining network separation between the public and private environments.
B. AWS Direct Connect provides a more consistent network experience than Internet-based connections.
C. AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS.
D. AWS Direct Connect reduces your network costs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
By using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space, while maintaining network separation between the public and private environments.
http://aws.amazon.com/directconnect/#details

QUESTION 163
An organization is setting up an application on AWS to have both High Availability (HA) and Disaster Recovery (DR). The organization wants to have both Recovery point objective (RPO) and Recovery time objective (RTO) of 10 minutes.

Which of the below mentioned service configurations does not help the organization achieve the said RPO and RTO?

A. Take a snapshot of the data every 10 minutes and copy it to the other region.
B. Use an elastic IP to assign to a running instance and use Route 53 to map the user's domain with that IP.
C. Create ELB with multi-region routing to allow automated failover when required.
D. Use an AMI copy to keep the AMI available in other regions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS provides an on demand, scalable infrastructure. AWS EC2 allows the user to launch On- Demand instances and the organization should create an AMI of the running instance. Copy the AMI to another region to enable Disaster Recovery (DR) in case of region failure. The organization should also use EBS for persistent storage and take a snapshot every 10 minutes to meet Recovery time objective (RTO). They should also setup an elastic IP and use it with Route 53 to route requests to the same IP. When one of the instances fails the organization can launch new instances and assign the same EIP to a new instance to achieve High Availability (HA). The ELB works only for a particular region and does not route requests across regions.
Reference: http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf

QUESTION 164 An organization is having an application which can start and stop an EC2 instance as per schedule. The organization needs the MAC address of the instance to be registered with its software. The instance is launched in EC2-CLASSIC.

How can the organization update the MAC registration every time an instance is booted?

A. The organization should write a boot strapping script which will get the MAC address from the instance metadata and use that script to register with the application.
B. The organization should provide a MAC address as a part of the user data. Thus, whenever the instance is booted the script assigns the fixed MAC address to that instance.
C. The instance MAC address never changes. Thus, it is not required to register the MAC address every time.
D. AWS never provides a MAC address to an instance; instead the instance ID is used for identifying the instance for any software registration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS provides an on demand, scalable infrastructure. AWS EC2 allows the user to launch On- Demand instances. AWS does not provide a fixed MAC address to the instances launched in EC2-CLASSIC. If the instance is launched as a part of EC2-VPC, it can have an ENI which can have a fixed MAC. However, with EC2-CLASSIC, every time the instance is started or stopped it will have a new MAC address. To get this MAC, the organization can run a script on boot which can fetch the instance metadata and get the MAC address from that instance metadata. Once the MAC is received, the organization can register that MAC with the software. Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AESDG-chapter-instancedata.html

QUESTION 165
Does Amazon RDS API provide actions to modify DB instances inside a VPC and associate them with DB Security Groups?

A. Yes, Amazon does this but only for MySQL RDS.

B. Yes
C. No
D. Yes, Amazon does this but only for Oracle RDS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use the action Modify DB Instance, available in the Amazon RDS API, to pass values for the parameters DB Instance Identifier and DB Security Groups specifying the instance ID and the DB Security Groups you want your instance to be part of.

Reference: http://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_ModifyDBInstance.html

QUESTION 166
An organization is setting up a backup and restore system in AWS of their in premise system. The organization needs High Availability(HA) and Disaster Recovery(DR) but is okay to have a longer recovery time to save costs.

Which of the below mentioned setup options helps achieve the objective of cost saving as well as DR in the most effective way?

A. Setup pre-configured servers and create AMIs. Use EIP and Route 53 to quickly switch over to AWS from in premise.
B. Setup the backup data on S3 and transfer data to S3 regularly using the storage gateway.
C. Setup a small instance with AutoScaling; in case of DR start diverting all the load to AWS from on premise.
D. Replicate on premise DB to EC2 at regular intervals and setup a scenario similar to the pilot light.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS has many solutions for Disaster Recovery(DR) and High Availability(HA). When the organization wants to have HA and DR but are okay to have a longer recovery time they should select the option backup and restore with S3. The data can be sent to S3 using either Direct Connect, Storage Gateway or over the internet.
The EC2 instance will pick the data from the S3 bucket when started and setup the environment. This process takes longer but is very cost effective due to the low pricing of S3. In all the other options, the EC2 instance might be running or there will be AMI storage costs. Thus, it will be a costlier option. In this scenario the organization should plan appropriate tools to take a backup, plan the retention policy for data and setup security of the data.
http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf

QUESTION 167 By default, what is the maximum number of Cache Nodes you can run in Amazon ElastiCache?

A. 20
B. 50
C. 100
D. 200

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon ElastiCache, you can run a maximum of 20 Cache Nodes.
QUESTION 168
Does an AWS Direct Connect location provide access to Amazon Web Services in the region it is associated with as well as access to other US regions?

A. No, it provides access only to the region it is associated with.
B. No, it provides access only to the US regions other than the region it is associated with.
C. Yes, it provides access.

D. Yes, it provides access but only when there's just one Availability Zone in the region.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. For example, you can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US).

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION 169
Which of the following components of AWS Data Pipeline specifies the business logic of your data management?

A. Task Runner
B. Pipeline definition
C. AWS Direct Connect
D. Amazon Simple Storage Service 9Amazon S3)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A pipeline definition specifies the business logic of your data management.

Reference: http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html

QUESTION 170
What feature of the load balancing service attempts to force subsequent connections to a service to be redirected to the same node as long as it is online?

A. Node balance
B. Session retention
C. Session multiplexing
D. Session persistence

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Session persistence is a feature of the load balancing service. It attempts to force subsequent connections to a service to be redirected to the same node as long as it is online.

Reference: http://docs.rackspace.com/loadbalancers/api/v1.0/clb-devguide/content/Concepts-d1e233.html

QUESTION 171
What types of identities do Amazon Cognito identity pools support?
A. They support both authenticated and unauthenticated identities.
B. They support only unauthenticated identities.
C. They support neither authenticated nor unauthenticated identities.
D. They support only authenticated identities.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Cognito identity pools support both authenticated and unauthenticated identities. Authenticated identities belong to users who are authenticated by a public login provider or your own backend authentication process. Unauthenticated identities typically belong to guest users.

Reference: http://docs.aws.amazon.com/cognito/devguide/identity/identity-pools/

QUESTION 172 In IAM, which of the following is true of temporary security credentials?

A. Once you issue temporary security credentials, they cannot be revoked.
B. None of these are correct.
C. Once you issue temporary security credentials, they can be revoked only when the virtual MFA device is used.
D. Once you issue temporary security credentials, they can be revoked.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Temporary credentials in IAM are valid throughout their defined duration of time and hence can't be revoked. However, because permissions are evaluated each time an AWS request is made using the credentials, you can achieve the effect of revoking the credentials by changing the permissions for the credentials even after they have been issued. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_disable-perms.html

QUESTION 173 The CFO of a company wants to allow one of his employees to view only the AWS usage report page.

Which of the below mentioned IAM policy statements allows the user to have access to the AWS usage report page?

A. "Effect": "Allow", "Action": ["Describe"], "Resource": "Billing"
B. "Effect": "Allow", "Action": ["aws-portal: ViewBilling"], "Resource": "*"
C. "Effect": "Allow", "Action": ["aws-portal: ViewUsage"], "Resource": "*"
D. "Effect": "Allow", "Action": ["AccountUsage], "Resource": "*"

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. If the CFO wants to allow only AWS usage report page access, the policy for that IAM user will be as given below:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow", "Action": [
"aws-portal:ViewUsage"
],
"Resource": "*"
}
]
}
```

http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-permissions-ref.html

QUESTION 174 In Amazon VPC, what is the default maximum number of BGP advertised routes allowed per route table?

A. 15
B. 100
C. 5
D. 10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The maximum number of BGP advertised routes allowed per route table is 100.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html

QUESTION 175
An organization has created 5 IAM users. The organization wants to give them the same login ID but different passwords. How can the organization achieve this?

A. The organization should create each user in a separate region so that they have their own URL to login
B. The organization should create a separate login ID but give the IAM users the same alias so that each one can login with their alias
C. It is not possible to have the same login ID for multiple IAM users of the same account
D. The organization should create various groups and add each user with the same login ID to different groups. The user can login with their own group ID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services.
Whenever the organization is creating an IAM user, there should be a unique ID for each user. It is not possible to have the same login ID for multiple users. The names of users, groups, roles, instance profiles must be alphanumeric, including the following common characters: plus (+), equal (=), comma (,), period (.), at (@), and dash (-). http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_SettingUpUser.html

QUESTION 176
The user has provisioned the PIOPS volume with an EBS optimized instance.
Generally speaking, in which I/O chunk should the bandwidth experienced by the user be measured by AWS?

A. 128 KB
B. 256 KB
C. 64 KB
D. 32 KB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IOPS are input/output operations per second. Amazon EBS measures each I/O operation per second (that is 256 KB or smaller) as one IOPS. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-io-characteristics.html
QUESTION 177
A user is planning to use EBS for his DB requirement. The user already has an EC2 instance running in the VPC private subnet. How can the user attach the EBS volume to a running instance?

A. The user can create EBS in the same zone as the subnet of instance and attach that EBS to instance.
B. It is not possible to attach an EBS to an instance running in VPC until the instance is stopped.

C. The user can specify the same subnet while creating EBS and then attach it to a running instance.
D. The user must create EBS within the same VPC and then attach it to a running instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC. The VPC is always specific to a region. The user can create a VPC which can span multiple Availability Zones by adding one or more subnets in each Availability Zone. The instance launched will always be in the same availability zone of the respective subnet. When creating an EBS the user cannot specify the subnet or VPC. However, the user must create the EBS in the same zone as the instance so that it can attach the EBS volume to the running instance.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPCSubnet

QUESTION 178
An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the webserver on a single VPC instance such that it allows the internet traffic as well as the back-end management traffic. The organization wants to make so that the back end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing webserver will have an IP address which can receive traffic from all the internet IPs.

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

A. It is not possible to have two IP addresses for a single instance.
B. The organization should create two network interfaces with the same subnet and security group to assign separate IPs to each network interface.
C. The organization should create two network interfaces with separate subnets so one instance can have two subnets and the respective security groups for controlled access.
D. The organization should launch an instance with two separate subnets using the same network interface which allows to have a separate CIDR as well as security groups.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. An Elastic Network Interface (ENI) is a virtual network interface that the user can attach to an instance in a VPC. The user can create a management network using two separate network interfaces. For the present scenario it is required that the secondary network interface on the instance handles the public facing traffic and the primary network interface handles the back-end management traffic and it is connected to a separate subnet in the VPC that has more restrictive access controls. The public facing interface, which may or may not be behind a load balancer, has an associated security group to allow access to the server from the internet while the private facing interface has an associated security group allowing SSH access only from an allowed range of IP addresses either within the VPC or from the internet, a private subnet within the VPC or a virtual private gateway.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 179 A user is trying to create a vault in AWS Glacier. The user wants to enable notifications.

In which of the below mentioned options can the user enable the notifications from the AWS console?

A. Glacier does not support the AWS console
B. Archival Upload Complete
C. Vault Upload Job Complete
D. Vault Inventory Retrieval Job Complete

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
From AWS console the user can configure to have notifications sent to Amazon Simple Notifications Service (SNS). The user can select specific jobs that, on completion, will trigger the notifications such as Vault Inventory Retrieval Job Complete and Archive Retrieval Job Complete.
http://docs.aws.amazon.com/amazonglacier/latest/dev/configuring-notifications-console.html

QUESTION 180

An organization is purchasing licensed software. The software license can be registered only to a specific MAC Address. The organization is going to host the software in the AWS environment.
How can the organization fulfil the license requirement as the MAC address changes every time an instance is started/stopped/terminated?

A. It is not possible to have a fixed MAC address with AWS.
B. The organization should use VPC with the private subnet and configure the MAC address with that subnet.
C. The organization should use VPC with an elastic network interface which will have a fixed MAC Address.
D. The organization should use VPC since VPC allows to configure the MAC address for each EC2 instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. An Elastic Network Interface (ENI) is a virtual network interface that the user can attach to an instance in a VPC. An ENI can include attributes such as: a primary private IP address, one or more secondary private IP addresses, one elastic IP address per private IP address, one public IP address, one or more security groups, a MAC address, a source/destination check flag, and a description. The user can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. The attributes of a network interface follow the network interface as it is attached or detached from an instance and reattached to another instance. Thus, the user can maintain a fixed MAC using the network interface.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 181

ABC has three separate departments and each department has their own AWS accounts. The HR department has created a file sharing site where all the on roll employees' data is uploaded. The Admin department uploads data about the employee presence in the office to their DB hosted in the VPC. The Finance department needs to access data from the HR department to know the on roll employees to calculate the salary based on the number of days that an employee is present in the office.
How can ABC setup this scenario?

A. It is not possible to configure VPC peering since each department has a separate AWS account.
B. Setup VPC peering for the VPCs of Admin and Finance.
C. Setup VPC peering for the VPCs of Finance and HR as well as between the VPCs of Finance and Admin.D. Setup VPC peering for the VPCs of Admin and HR

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. A VPC peering connection allows the user to route traffic between the peer VPCs using private IP addresses as if they are a part of the same network. This is helpful when one VPC from the same or different AWS account wants to connect with resources of the other VPC.
http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#three-vpcs-full-access.

QUESTION 182

An organization is undergoing a security audit. The auditor wants to view the AWS VPC configurations as the organization has hosted all the applications in the AWS VPC. The auditor is from a remote place and wants to have access to AWS to view all the VPC records.

How can the organization meet the expectations of the auditor without compromising on the security of their AWS infrastructure?

A. The organization should not accept the request as sharing the credentials means compromising on security.
B. Create an IAM role which will have read only access to all EC2 services including VPC and assign that role to the auditor.
C. Create an IAM user who will have read only access to the AWS VPC and share those credentials with the auditor.
D. The organization should create an IAM user with VPC full access but set a condition that will not allow to modify anything if the request is from any IP other than the organization's data center.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC. The VPC also works with IAM and the organization can create IAM users who have access to various VPC services. If an auditor wants to have access to the AWS VPC to verify the rules, the organization should be careful before sharing any data which can allow making updates to the AWS infrastructure. In this scenario it is recommended that the organization creates an IAM user who will have read only access to the VPC. Share the above mentioned credentials with the auditor as it cannot harm the organization. The sample policy is given below:

```
{
"Effect":"Allow", "Action": [ "ec2:DescribeVpcs", "ec2:DescribeSubnets",
"ec2: DescribeInternetGateways", "ec2:DescribeCustomerGateways", "ec2:DescribeVpnGateways", "ec2:DescribeVpnConnections", "ec2:DescribeRouteTables", "ec2:DescribeAddresses", "ec2:DescribeSecurityGroups",
"ec2:DescribeNetworkAcls", "ec2:DescribeDhcpOptions", "ec2:DescribeTags", "ec2:DescribeInstances"
],
"Resource":"*"
}
```

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

QUESTION 183 What is the maximum length for an instance profile name in AWS IAM?

A. 512 characters
B. 128 characters
C. 1024 charactersD. 64 characters

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The maximum length for an instance profile name is 128 characters.
http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

QUESTION 184
Cognito Sync is an AWS service that you can use to synchronize user profile data across mobile devices without requiring your own backend. When the device is online, you can synchronize data.

If you also set up push sync, what does it allow you to do?

A. Notify other devices that a user profile is available across multiple devices
B. Synchronize user profile data with less latency
C. Notify other devices immediately that an update is available
D. Synchronize online data faster

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cognito Sync is an AWS service that you can use to synchronize user profile data across mobile devices without requiring your own backend. When the device is online, you can synchronize data, and if you have also set up push sync, notify other devices immediately that an update is available. http://docs.aws.amazon.com/cognito/devguide/sync/

QUESTION 185
An organization is planning to create a secure scalable application with AWS VPC and ELB. The organization has two instances already running and each instance has an ENI attached to it in addition to a primary network interface. The primary network interface and additional ENI both have an elastic IP attached to it.
If those instances are registered with ELB and the organization wants ELB to send data to a particular EIP of the instance, how can they achieve this?

A. The organization should ensure that the IP which is required to receive the ELB traffic is attached to a primary network interface.
B. It is not possible to attach an instance with two ENIs with ELB as it will give an IP conflict error.
C. The organization should ensure that the IP which is required to receive the ELB traffic is attached to an additional ENI.
D. It is not possible to send data to a particular IP as ELB will send to any one EIP.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Within this virtual private cloud, the user can launch AWS resources, such as an ELB, and EC2 instances. There are two ELBs available with VPC: internet facing and internal (private) ELB. For the internet facing ELB it is required that the ELB should be in a public subnet. When the user registers a multi-homed instance (an instance that has an Elastic Network Interface (ENI) attached) with a load balancer, the load balancer will route the traffic to the IP address of the primary network interface (eth0).
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/gs-ec2VPC.html

QUESTION 186
In Amazon Cognito, your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new _____ for the user and a set of temporary, limited-privilege AWS credentials.

A. Cognito Key Pair
B. Cognito API
C. Cognito ID
D. Cognito SDK

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Your mobile app authenticates with the identity provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new Cognito ID for the user and a set of temporary, limited-privilege AWS credentials. http://aws.amazon.com/cognito/faqs/

QUESTION 187 What is the maximum length for a certificate
ID in AWS IAM?

A. 1024 characters
B. 512 characters
C. 64 characters
D. 128 characters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The maximum length for a certificate ID is 128 characters. http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

QUESTION 188
A user is trying to create a PIOPS EBS volume with 3 GB size and 90 IOPS. Will AWS create the volume?
A. No, since the PIOPS and EBS size ratio is less than 30
B. Yes, since the ratio between EBS and IOPS is less than 30
C. No, the EBS size is less than 4GB
D. Yes, since PIOPS is higher than 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
A Provisioned IOPS (SSD) volume can range in size from 4 GiB to 16 TiB and you can provision up to 20,000 IOPS per volume.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops

QUESTION 189 If a single condition within an IAM policy includes multiple values for one key, it will be evaluated using a logical______.

A. OR
B. NAND
C. NOR
D. AND

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If a single condition within an IAM policy includes multiple values for one key, it will be evaluated using a logical OR.
http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

QUESTION 190 Which of the following cache engines does Amazon ElastiCache support?

A. Amazon ElastiCache supports Memcached and Redis.
B. Amazon ElastiCache supports Redis and WinCache.
C. Amazon ElastiCache supports Memcached and Hazelcast.
D. Amazon ElastiCache supports Memcached only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The cache engines supported by Amazon ElastiCache are Memcached and Redis.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/SelectEngine.html

QUESTION 191 You have been given the task to define multiple AWS Data Pipeline schedules for different activities in the same pipeline.

Which of the following would successfully accomplish this task?

A. Creating multiple pipeline definition files
B. Defining multiple pipeline definitions in your schedule objects file and associating the desired schedule to the correct activity via its schedule field
C. Defining multiple schedule objects in your pipeline definition file and associating the desired schedule to the correct activity via its schedule fieldD. Defining multiple schedule objects in the schedule field

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To define multiple schedules for different activities in the same pipeline, in AWS Data Pipeline, you should define multiple schedule objects in your pipeline definition file and associate the desired schedule to the correct activity via its schedule field. As an example of this, it could allow you to define a pipeline in which log files are stored in Amazon S3 each hour to drive generation of an aggregate report once a day. https://aws.amazon.com/datapipeline/faqs/

QUESTION 192 In a VPC, can you modify a set of DHCP options after you create them?

A. Yes, you can modify a set of DHCP options within 48 hours after creation and there are no VPCs associated with them.
B. Yes, you can modify a set of DHCP options any time after you create them.
C. No, you can't modify a set of DHCP options after you create them.
D. Yes, you can modify a set of DHCP options within 24 hours after creation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
After you create a set of DHCP options, you can't modify them. If you want your VPC to use a different set of DHCP options, you must create a new set and associate them with your VPC. You can also set up your VPC to use no DHCP options at all.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html

QUESTION 193 A bucket owner has allowed another account's IAM users to upload or access objects in his bucket. The IAM user of Account A is trying to access an object created by the IAM user of account B. What will happen in this scenario?

A. It is not possible to give permission to multiple IAM users
B. AWS S3 will verify proper rights given by the owner of Account A, the bucket owner as well as by the IAM user B to the object
C. The bucket policy may not be created as S3 will give error due to conflict of Access RightsD. It is not possible that the IAM user of one account accesses objects of the other IAM user

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If a IAM user is trying to perform some action on an object belonging to another AWS user's bucket, S3 will verify whether the owner of the IAM user has given sufficient permission to him. It also verifies the policy for the bucket as well as the policy defined by the object owner. http://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-auth-workflow-object-operation.html

QUESTION 194
Which statement is NOT true about a stack which has been created in a Virtual Private Cloud (VPC) in AWS OpsWorks?

A. Subnets whose instances cannot communicate with the Internet are referred to as public subnets.
B. Subnets whose instances can communicate only with other instances in the VPC and cannot communicate directly with the Internet are referred to as private subnets.
C. All instances in the stack should have access to any package repositories that your operating system depends on, such as the Amazon Linux or Ubuntu Linux repositories.
D. Your app and custom cookbook repositories should be accessible for all instances in the stack.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:
In AWS OpsWorks, you can control user access to a stack's instances by creating it in a virtual private cloud (VPC). For example, you might not want users to have direct access to your stack's app servers or databases and instead require that all public traffic be channeled through an Elastic Load Balancer. A VPC consists of one or more subnets, each of which contains one or more instances. Each subnet has an associated routing table that directs outbound traffic based on its destination IP address. Instances within a VPC can generally communicate with each other, regardless of their subnet. Subnets whose instances can communicate with the Internet are referred to as public subnets. Subnets whose instances can communicate only with other instances in the VPC and cannot communicate directly with the Internet are referred to as private subnets. AWS OpsWorks requires the VPC to be configured so that every instance in the stack, including instances in private subnets, has access to the following endpoints:
The AWS OpsWorks service, https://opsworks-instance-service.us-east-1.amazonaws.com .
Amazon S3
The package repositories for Amazon Linux or Ubuntu 12.04 LTS, depending on which operating system you specify.
Your app and custom cookbook repositories.
http://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks-vpc.html#workingstacks-vpc-basics

QUESTION 195
An organization has hosted an application on the EC2 instances. There will be multiple users connecting to the instance for setup and configuration of application. The organization is planning to implement certain security best practices.

Which of the below mentioned pointers will not help the organization achieve better security arrangement?

A. Allow only IAM users to connect with the EC2 instances with their own secret access key.
B. Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.
C. Apply the latest patch of OS and always keep it updated.
D. Disable the password based login for all the users. All the users should use their own keys to connect with the instance securely.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since AWS is a public cloud any application hosted on EC2 is prone to hacker attacks. It becomes extremely important for a user to setup a proper security mechanism on the EC2 instances. A few of the security measures are listed below:
Always keep the OS updated with the latest patch
Always create separate users with in OS if they need to connect with the EC2 instances, create their keys and disable their password
Create a procedure using which the admin can revoke the access of the user when the business work on the EC2 instance is completed. Lock down unnecessary ports.
Audit any proprietary applications that the user may be running on the EC2 instance Provide temporary escalated privileges, such as sudo for users who need to perform occasional privileged tasks The
IAM is useful when users are required to work with AWS resources and actions, such as launching an instance. It is not useful to connect (RDP / SSH) with an instance.
http://aws.amazon.com/articles/1233/

QUESTION 196 By default, temporary security credentials for an IAM user are valid for a maximum of 12 hours, but you can request a duration as long as
_________ hours.

A. 24
B. 36
C. 10
D. 48

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By default, temporary security credentials for an IAM user are valid for a maximum of 12 hours, but you can request a duration as short as 15 minutes or as long as 36 hours.
http://docs.aws.amazon.com/STS/latest/UsingSTS/CreatingSessionTokens.html

QUESTION 197
What RAID method is used on the Cloud Block Storage back-end to implement a very high level of reliability and performance?

A. RAID 1 (Mirror)
B. RAID 5 (Blocks striped, distributed parity)
C. RAID 10 (Blocks mirrored and striped)
D. RAID 2 (Bit level striping)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cloud Block Storage back-end storage volumes employs the RAID 10 method to provide a very high level of reliability and performance. http://www.rackspace.com/knowledge_center/product-faq/cloud-block-storage

QUESTION 198
One of the AWS account owners faced a major challenge in June as his account was hacked and the hacker deleted all the data from his AWS account. This resulted in a major blow to the business.

Which of the below mentioned steps would not have helped in preventing this action?

A. Setup an MFA for each user as well as for the root account user.
B. Take a backup of the critical data to offsite / on premise.
C. Create an AMI and a snapshot of the data at regular intervals as well as keep a copy to separate regions.
D. Do not share the AWS access and secret access keys with others as well do not store it inside programs, instead use IAM roles.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS security follows the shared security model where the user is as much responsible as Amazon. If the user wants to have secure access to AWS while hosting applications on EC2, the first security rule to follow is to enable MFA for all users. This will add an added security layer. In the second step, the user should never give his access or secret access keys to anyone as well as store inside programs. The better solution is to use IAM roles. For critical data of the organization, the user should keep an offsite/ in premise backup which will help to recover critical data in case of security breach. It is recommended to have AWS AMIs and snapshots as well as keep them at other regions so that they will help in the DR scenario. However, in case of a data security breach of the account they may not be very helpful as hacker can delete that.
Therefore, creating an AMI and a snapshot of the data at regular intervals as well as keep a copy to separate regions, would not have helped in preventing this action.

QUESTION 199
With Amazon Elastic MapReduce (Amazon EMR) you can analyze and process vast amounts of data. The cluster is managed using an open-source framework called Hadoop. You have set up an application to run Hadoop jobs. The application reads data from DynamoDB and generates a temporary file of 100 TBs. The whole process runs for 30 minutes and the output of the job is stored to S3.

Which of the below mentioned options is the most cost effective solution in this case?

A. Use Spot Instances to run Hadoop jobs and configure them with EBS volumes for persistent data storage.
B. Use Spot Instances to run Hadoop jobs and configure them with ethereal storage for output file storage.
C. Use an on demand instance to run Hadoop jobs and configure them with EBS volumes for persistent storage.
D. Use an on demand instance to run Hadoop jobs and configure them with ephemeral storage for output file storage.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS EC2 Spot Instances allow the user to quote his own price for the EC2 computing capacity. The user can simply bid on the spare Amazon EC2 instances and run them whenever his bid exceeds the current Spot Price. The Spot Instance pricing model complements the On-Demand and Reserved Instance pricing models, providing potentially the most cost-effective option for obtaining compute capacity, depending on the application. The only challenge with a Spot Instance is data persistence as the instance can be terminated whenever the spot price exceeds the bid price. In the current scenario a Hadoop job is a temporary job and does not run for a longer period. It fetches data from a persistent DynamoDB. Thus, even if the instance gets terminated there will be no data loss and the job can be re-run. As the output files are large temporary files, it will be useful to store data on ethereal storage for cost savings.
http://aws.amazon.com/ec2/purchasing-options/spot-instances/

QUESTION 200
In Amazon SNS, to send push notifications to mobile devices using Amazon SNS and ADM, you need to obtain the following, except:
A. Device token
B. Client ID
C. Registration ID
D. Client secret

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To send push notifications to mobile devices using Amazon SNS and ADM, you need to obtain the following: Registration ID and Client secret. http://docs.aws.amazon.com/sns/latest/dg/SNSMobilePushPrereq.html

QUESTION 201
True or False: "In the context of Amazon ElastiCache, from the application's point of view, connecting to the cluster configuration endpoint is no different than connecting directly to an individual cache node."

A. True, from the application's point of view, connecting to the cluster configuration endpoint is no different than connecting directly to an individual cache node since, each has a unique node identifier.
B. True, from the application's point of view, connecting to the cluster configuration endpoint is no different than connecting directly to an individual cache node.
C. False, you can connect to a cache node, but not to a cluster configuration endpoint.
D. False, you can connect to a cluster configuration endpoint, but not to a cache node.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is true. From the application's point of view, connecting to the cluster configuration endpoint is no different than connecting directly to an individual cache node. In the process of connecting to cache nodes, the application resolves the configuration endpoint's DNS name. Because the configuration endpoint maintains CNAME entries for all of the cache nodes, the DNS name resolves to one of the nodes; the client can then connect to that node.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/AutoDiscovery.HowAutoDiscoveryWorks.html

QUESTION 202
An organization is setting up a highly scalable application using Elastic Beanstalk.
They are using Elastic Load Balancing (ELB) as well as a Virtual Private Cloud (VPC) with public and private subnets. They have the following requirements:

```
- All the EC2 instances should have a private IP
- All the EC2 instances should receive data via the ELB's.
```

Which of these will not be needed in this setup?

A. Launch the EC2 instances with only the public subnet.
B. Create routing rules which will route all inbound traffic from ELB to the EC2 instances.
C. Configure ELB and NAT as a part of the public subnet only.
D. Create routing rules which will route all outbound traffic from the EC2 instances through NAT.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. If the organization wants the Amazon EC2 instances to have a private IP address, he should create a public and private subnet for VPC in each Availability Zone (this is an AWS Elastic Beanstalk requirement). The organization should add their public resources, such as ELB and NAT to the public subnet, and AWC Elastic Beanstalk will assign them unique elastic IP addresses (a static, public IP address). The organization should launch Amazon EC2 instances in a private subnet so that AWS Elastic Beanstalk assigns them non-routable private IP addresses. Now the organization should configure route tables with the following rules:
▪ route all inbound traffic from ELB to EC2 instances ▪ route all outbound
traffic from EC2 instances through NAT
http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo-vpc.html
QUESTION 203
An EC2 instance that performs source/destination checks by default is launched in a private VPC subnet. All security, NACL, and routing definitions are configured as expected. A custom NAT instance is launched.

Which of the following must be done for the custom NAT instance to work?

A. The source/destination checks should be disabled on the NAT instance.
B. The NAT instance should be launched in public subnet.
C. The NAT instance should be configured with a public IP address.
D. The NAT instance should be configured with an elastic IP address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#EIP_DisableSrcDestCheck

QUESTION 204
An organization has created multiple components of a single application for compartmentalization. Currently all the components are hosted on a single EC2 instance. Due to security reasons the organization wants to implement two separate SSLs for the separate modules although it is already using VPC.

How can the organization achieve this with a single instance?

A. You have to launch two instances each in a separate subnet and allow VPC peering for a single IP.
B. Create a VPC instance which will have multiple network interfaces with multiple elastic IP addresses.
C. Create a VPC instance which will have both the ACL and the security group attached to it and have separate rules for each IP address.
D. Create a VPC instance which will have multiple subnets attached to it and each will have a separate IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. With VPC the user can specify multiple private IP addresses for his instances.
The number of network interfaces and private IP addresses that a user can specify for an instance depends on the instance type. With each network interface the organization can assign an EIP. This scenario helps when the user wants to host multiple websites on a single EC2 instance by using multiple SSL certificates on a single server and associating each certificate with a specific EIP address. It also helps in scenarios for operating network appliances, such as firewalls or load balancers that have multiple private IP addresses for each network interface. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html

QUESTION 205
An organization is making software for the CIA in USA. CIA agreed to host the application on AWS but in a secure environment. The organization is thinking of hosting the application on the AWS GovCloud region. Which of the below mentioned difference is not correct when the organization is hosting on the AWS GovCloud in comparison with the AWS standard region?

A. The billing for the AWS GovCLoud will be in a different account than the Standard AWS account.
B. GovCloud region authentication is isolated from Amazon.com.
C. Physical and logical administrative access only to U.S. persons.
D. It is physically isolated and has logical network isolation from all the other regions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS GovCloud (US) is an isolated AWS region designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) Region adheres to the U.S. International Traffic in Arms Regulations (ITAR) requirements. It has added advantages, such as:
Restricting physical and logical administrative access to U.S. persons only There will be a separate AWS GovCloud (US) credentials, such as access key and secret access key than the standard AWS account
The user signs in with the IAM user name and password
The AWS GovCloud (US) Region authentication is completely isolated from Amazon.com If the organization is planning to host on EC2 in AWS GovCloud then it will be billed to standard AWS account of organization since AWS GovCloud billing is linked with the standard AWS account and is not be billed separately. http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/whatis.html

QUESTION 206 How does in-memory caching improve the performance of applications in ElastiCache?

A. It improves application performance by deleting the requests that do not contain frequently accessed data.
B. It improves application performance by implementing good database indexing strategies.
C. It improves application performance by using a part of instance RAM for caching important data.
D. It improves application performance by storing critical pieces of data in memory for low-latency access.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon ElastiCache, in-memory caching improves application performance by storing critical pieces of data in memory for low-latency access. Cached information may include the results of I/O-intensive database queries or the results of computationally intensive calculations. http://aws.amazon.com/elasticache/faqs/#g4

QUESTION 207 A user is thinking to use
EBS PIOPS volume.

Which of the below mentioned options is a right use case for the PIOPS EBS volume?

A. Analytics
B. System boot volume
C. Mongo DB
D. Log processing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Provisioned IOPS volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput. Provisioned IOPS volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency in random access I/O throughput business applications, database workloads, such as NoSQL DB, RDBMS, etc.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

QUESTION 208 How can a user list the IAM Role configured as a part of
the launch config?

A. as-describe-launch-configs -iam-profile
B. as-describe-launch-configs -show-long
C. as-describe-launch-configs -iam-role
D. as-describe-launch-configs -role

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
As-describe-launch-configs describes all the launch config parameters created by the AWS account in the specified region. Generally, it returns values, such as Launch Config name, Instance Type and AMI ID. If the user wants additional parameters, such as the IAM Profile used in the config, he has to run command: as-describe-launch-configs --show-long

QUESTION 209
An organization is setting up a multi-site solution where the application runs on premise as well as on AWS to achieve the minimum recovery time objective(RTO).

Which of the below mentioned configurations will not meet the requirements of the multi-site solution scenario?

A. Configure data replication based on RTO.
B. Keep an application running on premise as well as in AWS with full capacity.
C. Setup a single DB instance which will be accessed by both sites.
D. Setup a weighted DNS service like Route 53 to route traffic across sites.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

AWS has many solutions for DR (Disaster recovery) and HA (High Availability). When the organization wants to have HA and DR with multi-site solution, it should setup two sites: one on premise and the other on AWS with full capacity. The organization should setup a weighted DNS service which can route traffic to both sites based on the weightage. When one of the sites fails it can route the entire load to another site. The organization would have minimal RTO in this scenario. If the organization setups a single DB instance, it will not work well in failover.

Instead they should have two separate DBs in each site and setup data replication based on RTO (recovery time objective) of the organization. http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf

QUESTION 210

Which of the following is true of an instance profile when an IAM role is created using the console?

A. The instance profile uses a different name.

B. The console gives the instance profile the same name as the role it corresponds to.

C. The instance profile should be created manually by a user.

D. The console creates the role and instance profile as separate actions.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon EC2 uses an instance profile as a container for an IAM role. When you create an IAM role using the console, the console creates an instance profile automatically and gives it the same name as the role it corresponds to. If you use the AWS CLI, API, or an AWS SDK to create a role, you create the role and instance profile as separate actions, and you might give them different names. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html

QUESTION 211 In the context of policies and permissions in AWS IAM, the Condition element is

____________.

A. crucial while writing the IAM policies

B. an optional element

C. always set to null

D. a mandatory element

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Condition element (or Condition block) lets you specify conditions for when a policy is in effect. The Condition element is optional.

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

QUESTION 212

Which of the following is true while using an IAM role to grant permissions to applications running on Amazon EC2 instances?

A. All applications on the instance share the same role, but different permissions.

B. All applications on the instance share multiple roles and permissions.

C. Multiple roles are assigned to an EC2 instance at a time.

D. Only one role can be assigned to an EC2 instance at a time.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Only one role can be assigned to an EC2 instance at a time, and all applications on the instance share the same role and permissions.

http://docs.aws.amazon.com/IAM/latest/UserGuide/role-usecase-ec2app.html

QUESTION 213

When using string conditions within IAM, short versions of the available comparators can be used instead of the more verbose ones.
streqi is the short version of the _______ string condition.

A. StringEqualsIgnoreCase
B. StringNotEqualsIgnoreCase
C. StringLikeStringEquals
D. StringNotEquals

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When using string conditions within IAM, short versions of the available comparators can be used instead of the more verbose versions. For instance, streqi is the short version of StringEqualsIgnoreCase that checks for the exact match between two strings ignoring their case. http://awsdocs.s3.amazonaws.com/SNS/20100331/sns-gsg-2010-03-31.pdf

QUESTION 214

Attempts, one of the three types of items associated with the schedule pipeline in the AWS Data Pipeline, provides robust data management.

Which of the following statements is NOT true about Attempts?

A. Attempts provide robust data management.
B. AWS Data Pipeline retries a failed operation until the count of retries reaches the maximum number of allowed retry attempts.
C. An AWS Data Pipeline Attempt object compiles the pipeline components to create a set of actionable instances.
D. AWS Data Pipeline Attempt objects track the various attempts, results, and failure reasons if applicable.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Attempts, one of the three types of items associated with a schedule pipeline in AWS Data Pipeline, provides robust data management. AWS Data Pipeline retries a failed operation. It continues to do so until the task reaches the maximum number of allowed retry attempts. Attempt objects track the various attempts, results, and failure reasons if applicable. Essentially, it is the instance with a counter. AWS Data Pipeline performs retries using the same resources from the previous attempts, such as Amazon EMR clusters and EC2 instances. http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-how-tasks-scheduled.html

QUESTION 215 Select the correct statement about
Amazon ElastiCache.

A. It makes it easy to set up, manage, and scale a distributed in-memory cache environment in the cloud.
B. It allows you to quickly deploy your cache environment only if you install software.
C. It does not integrate with other Amazon Web Services.
D. It cannot run in the Amazon Virtual Private Cloud (Amazon VPC) environment.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in memory cache environment in the cloud. It provides a high-performance, scalable, and cost- effective caching solution, while removing the complexity associated with deploying and managing a distributed cache environment. With ElastiCache, you can quickly deploy your cache environment, without having to provision hardware or install software.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/WhatIs.html

QUESTION 216

In Amazon RDS for PostgreSQL, you can provision up to 3TB storage and 30,000 IOPS per database instance. For a workload with 50% writes and 50% reads running on a cr1.8xlarge instance, you can realize over 25,000 IOPS for PostgreSQL. However, by provisioning more than this limit, you may be able to achieve:

A. higher latency and lower throughput.
B. lower latency and higher throughput.
C. higher throughput only.
D. higher latency only.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can provision up to 3TB storage and 30,000 IOPS per database instance. For a workload with 50% writes and 50% reads running on a cr1.8xlarge instance, you can realize over 25,000 IOPS for PostgreSQL. However, by provisioning more than this limit, you may be able to achieve lower latency and higher throughput. Your actual realized IOPS may vary from the amount you provisioned based on your database workload, instance type, and database engine choice.
https://aws.amazon.com/rds/postgresql/

QUESTION 217 Which of the following cannot be done using
AWS Data Pipeline?

A. Create complex data processing workloads that are fault tolerant, repeatable, and highly available.
B. Regularly access your data where it's stored, transform and process it at scale, and efficiently transfer the results to another AWS service.
C. Generate reports over data that has been stored.
D. Move data between different AWS compute and storage services as well as on premise data sources at specified intervals.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services as well as on premise data sources at specified intervals. With AWS Data Pipeline, you can regularly access your data where it's stored, transform and process it at scale, and efficiently transfer the results to another AWS.
AWS Data Pipeline helps you easily create complex data processing workloads that are fault tolerant, repeatable, and highly available. AWS Data Pipeline also allows you to move and process data that was previously locked up in on premise data silos. http://aws.amazon.com/datapipeline/

QUESTION 218
AWS Direct Connect itself has NO specific resources for you to control access to. Therefore, there are no AWS Direct Connect Amazon Resource Names (ARNs) for you to use in an Identity and Access Management (IAM) policy.

With that in mind, how is it possible to write a policy to control access to AWS Direct Connect actions?

A. You can leave the resource name field blank.
B. You can choose the name of the AWS Direct Connection as the resource.
C. You can use an asterisk (*) as the resource.
D. You can create a name for the resource.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect itself has no specific resources for you to control access to. Therefore, there are no AWS Direct Connect ARNs for you to use in an IAM policy. You use an asterisk (*) as the resource when writing a policy to control access to AWS Direct Connect actions. http://docs.aws.amazon.com/directconnect/latest/UserGuide/using_iam.html

QUESTION 219 Identify an application that polls AWS Data Pipeline for tasks and then
performs those tasks.

A. A task executor
B. A task deployer
C. A task runner
D. A task optimizer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A task runner is an application that polls AWS Data Pipeline for tasks and then performs those tasks. You can either use Task Runner as provided by AWS Data Pipeline, or create a custom Task Runner application.
Task Runner is a default implementation of a task runner that is provided by AWS Data Pipeline. When Task Runner is installed and configured, it polls AWS Data Pipeline for tasks associated with pipelines that you have activated. When a task is assigned to Task Runner, it performs that task and reports its status back to AWS Data Pipeline. If your workflow requires non-default behavior, you'll need to implement that functionality in a custom task runner.
http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-how-remote-taskrunner-client.html

QUESTION 220
With respect to AWS Lambda permissions model, at the time you create a Lambda function, you specify an IAM role that AWS Lambda can assume to execute your Lambda function on your behalf. This role is also referred to as the________role.

A. configuration
B. execution
C. delegation
D. dependency

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Regardless of how your Lambda function is invoked, AWS Lambda always executes the function. At the time you create a Lambda function, you specify an IAM role that AWS Lambda can assume to execute your Lambda function on your behalf. This role is also referred to as the execution role.
http://docs.aws.amazon.com/lambda/latest/dg/lambda-dg.pdf

QUESTION 221 Within an IAM policy, can you add an IfExists condition at the end of a Null condition?

A. Yes, you can add an IfExists condition at the end of a Null condition but not in all Regions.
B. Yes, you can add an IfExists condition at the end of a Null condition depending on the condition.
C. No, you cannot add an IfExists condition at the end of a Null condition.
D. Yes, you can add an IfExists condition at the end of a Null condition.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Within an IAM policy, IfExists can be added to the end of any condition operator except the Null condition. It can be used to indicate that conditional comparison needs to happen if the policy key is present in the context of a request; otherwise, it can be ignored. http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

QUESTION 222 Regarding Identity and Access Management (IAM), Which type of special account belonging to your application allows your code to access Google services programmatically?

A. Service account
B. Simple Key
C. OAuth

D. Code account

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A service account is a special Google account that can be used by applications to access Google services programmatically. This account belongs to your application or a virtual machine (VM), instead of to an individual end user. Your application uses the service account to call the Google API of a service, so that the users aren't directly involved.
A service account can have zero or more pairs of service account keys, which are used to authenticate to Google. A service account key is a public/private key pair generated by Google. Google retains the public key, while the user is given the private key. https://cloud.google.com/iam/docs/service-accounts

QUESTION 223 IAM users do not have permission to create Temporary Security Credentials for federated users and roles by default. In contrast, IAM users can call __________ without the need of any special permissions

A. GetSessionName
B. GetFederationToken
C. GetSessionToken
D. GetFederationName

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Currently the STS API command GetSessionToken is available to every IAM user in your account without previous permission. In contrast, the GetFederationToken command is restricted and explicit permissions need to be granted so a user can issue calls to this particular Action. http://docs.aws.amazon.com/STS/latest/UsingSTS/STSPermission.html

QUESTION 224
An organization is planning to use NoSQL DB for its scalable data needs. The organization wants to host an application securely in AWS VPC.
What action can be recommended to the organization?

A. The organization should setup their own NoSQL cluster on the AWS instance and configure route tables and subnets.
B. The organization should only use a DynamoDB because by default it is always a part of the default subnet provided by AWS.
C. The organization should use a DynamoDB while creating a table within the public subnet.
D. The organization should use a DynamoDB while creating a table within a private subnet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Currently VPC does not support DynamoDB. Thus, if the user wants to implement VPC, he has to setup his own NoSQL DB within the VPC. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

QUESTION 225 What happens when Dedicated instances are launched into a VPC?

A. If you launch an instance into a VPC that has an instance tenancy of dedicated, you must manually create a Dedicated instance.
B. If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is created as a Dedicated instance, only based on the tenancy of the instance.
C. If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is automatically a Dedicated instance, regardless of the tenancy of the instance.
D. None of these are true.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is automatically a Dedicated instance, regardless of the tenancy of the instance.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html

QUESTION 226
An organization is setting up RDS for their applications. The organization wants to secure RDS access with VPC.

Which of the following options is not required while designing the RDS with VPC?

A. The organization must create a subnet group with public and private subnets. Both the subnets can be in the same or separate AZ.
B. The organization should keep minimum of one IP address in each subnet reserved for RDS failover.
C. If the organization is connecting RDS from the internet it must enable the VPC attributes DNS hostnames and DNS resolution.
D. The organization must create a subnet group with VPC using more than one subnet which are a part of separate AZs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources, such as RDS into a virtual network that the user has defined. Subnets are segments of a VPC's IP address range that the user can designate to a group of VPC resources based on security and operational needs. A DB subnet group is a collection of subnets (generally private) that the user can create in a VPC and assign to the RDS DB instances. A DB subnet group allows the user to specify a particular VPC when creating the DB instances.
Each DB subnet group should have subnets in at least two Availability Zones in a given region. If the RDS instance is required to be accessible from the internet the organization must enable the VPC attributes, DNS hostnames and DNS resolution. For each RDS DB instance that the user runs in a VPC, he should reserve at least one address in each subnet in the DB subnet group for use by Amazon RDS for recovery actions.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.html

QUESTION 227
You create a VPN connection, and your VPN device supports Border Gateway Protocol (BGP).
Which of the following should be specified to configure the VPN connection?

A. Classless routing
B. Classfull routing
C. Dynamic routing
D. Static routing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you create a VPN connection, you must specify the type of routing that you plan to use, which will depend upon on the make and model of your VPN devices. If your VPN device supports Border Gateway Protocol (BGP), you need to specify dynamic routing when you configure your VPN connection. If your device does not support BGP, you should specify static routing. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

QUESTION 228
An organization has developed an application which provides a smarter shopping experience. They need to show a demonstration to various stakeholders who may not be able to access the in premise application so they decide to host a demo version of the application on AWS.
Consequently, they will need a fixed elastic IP attached automatically to the instance when it is launched.

In this scenario which of the below mentioned options will not help assign the elastic IP automatically?

A. Write a script which will fetch the instance metadata on system boot and assign the public IP using that metadata.
B. Provide an elastic IP in the user data and setup a bootstrapping script which will fetch that elastic IP and assign it to the instance.

C. Create a controlling application which launches the instance and assigns the elastic IP based on the parameter provided when that instance is booted.
D. Launch instance with VPC and assign an elastic IP to the primary network interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: EC2 allows the user to launch On-Demand instances. If the organization is using an application temporarily only for demo purposes the best way to assign an elastic IP would be: Launch an instance with a VPC and assign an EIP to the primary network interface. This way on every instance start it will have the same IP
Create a bootstrapping script and provide it some metadata, such as user data which can be used to assign an EIP
Create a controller instance which can schedule the start and stop of the instance and provide an EIP as a parameter so that the controller instance can check the instance boot and assign an EIP The instance metadata gives the current instance data, such as the public/private IP. It can be of no use for assigning an EIP. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AESDG-chapter-instancedata.html

QUESTION 229
An organization is having a VPC for the HR department, and another VPC for the Admin department. The HR department requires access to all the instances running in the Admin VPC while the Admin department requires access to all the resources in the HR department.

How can the organization setup this scenario?

A. Setup VPC peering between the VPCs of Admin and HR.
B. Setup ACL with both VPCs which will allow traffic from the CIDR of the other VPC.
C. Setup the security group with each VPC which allows traffic from the CIDR of another VPC.
D. It is not possible to connect resources of one VPC from another VPC.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined.
A VPC peering connection allows the user to route traffic between the peer VPCs using private IP addresses as if they are a part of the same network. This is helpful when one VPC from the same or different AWS account wants to connect with resources of the other VPC.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

QUESTION 230 Can a Direct Connect link be connected directly to the Internet?

A. Yes, this can be done if you pay for it.
B. Yes, this can be done only for certain regions.
C. Yes
D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect is a network service that provides an alternative to using the Internet to utilize AWS cloud service. Hence, a Direct Connect link cannot be connected to the Internet directly. http://aws.amazon.com/directconnect/faqs/

QUESTION 231
ABC has created a multi-tenant Learning Management System (LMS). The application is hosted for five different tenants (clients) in the VPCs of the respective AWS accounts of the tenant. ABC wants to setup a centralized server which can connect with the LMS of each tenant upgrade if required. ABC also wants to ensure that one tenant VPC should not be able to connect to the other tenant VPC for security reasons.

How can ABC setup this scenario?

A. ABC has to setup one centralized VPC which will peer in to all the other VPCs of the tenants.

B. ABC should setup VPC peering with all the VPCs peering each other but block the IPs from CIDR of the tenant VPCs to deny them.
C. ABC should setup all the VPCs with the same CIDR but have a centralized VPC. This way only the centralized VPC can talk to the other VPCs using VPC peering.
D. ABC should setup all the VPCs meshed together with VPC peering for all VPCs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. A VPC peering connection allows the user to route traffic between the peer VPCs using private IP addresses as if they are a part of the same network.
This is helpful when one VPC from the same or different AWS account wants to connect with resources of the other VPC. The organization wants to setup that one VPC can connect with all the other VPCs but all other VPCs cannot connect among each other. This can be achieved by configuring VPC peering where one VPC is peered with all the other VPCs, but the other VPCs are not peered to each other. The VPCs are in the same or a separate AWS account and should not have overlapping CIDR blocks. http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#many-vpcs-full-acces

QUESTION 232 A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24.

What will happen in this scenario?

A. The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
B. The second subnet will be created
C. It will throw a CIDR overlaps error
D. It is not possible to create a subnet with the same CIDR as VPC

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 233 True or False: The Amazon ElastiCache clusters are not available for use in VPC at this time.

A. TRUE
B. True, but they are available only in the GovCloud.
C. True, but they are available only on request
D. FALSE

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Elasticache clusters can be run in an Amazon VPC. With Amazon VPC, you can define a virtual network topology and customize the network configuration to closely resemble a traditional network that you might operate in your own datacenter. You can now take advantage of the manageability, availability and scalability benefits of Amazon ElastiCache Clusters in your own isolated network. The same functionality of Amazon ElastiCache, including automatic failure detection, recovery, scaling, auto discovery, Amazon CloudWatch metrics, and software patching, are now available in Amazon VPC. http://aws.amazon.com/about-aws/whats-new/2012/12/20/amazon-elasticache-announces-support-for-amazon-vpc/

QUESTION 234 In Amazon Redshift, how many slices does a dw2.8xlarge node have?

A. 16
B. 8

C. 32
D. 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The disk storage for a compute node in Amazon Redshift is divided into a number of slices, equal to the number of processor cores on the node. For example, each DW1.XL compute node has two slices, and each DW2.8XL compute node has 32 slices. http://docs.aws.amazon.com/redshift/latest/dg/t_Distributing_data.html

QUESTION 235
Identify a true statement about using an IAM role to grant permissions to applications running on Amazon EC2 instances.

A. When AWS credentials are rotated; developers have to update only the root Amazon EC2 instance that uses their credentials.
B. When AWS credentials are rotated, developers have to update only the Amazon EC2 instance on which the password policy was applied and which uses their credentials.
C. When AWS credentials are rotated, you don't have to manage credentials and you don't have to worry about long-term security risks.
D. When AWS credentials are rotated, you must manage credentials and you should consider precautions for long-term security risks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Using IAM roles to grant permissions to applications that run on EC2 instances requires a bit of extra configuration. Because role credentials are temporary and rotated automatically, you don't have to manage credentials, and you don't have to worry about long-term security risks. http://docs.aws.amazon.com/IAM/latest/UserGuide/role-usecase-ec2app.html

QUESTION 236
Out of the striping options available for the EBS volumes, which one has the following disadvantage:
'Doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe.'?

A. Raid 1
B. Raid 0
C. RAID 1+0 (RAID 10)
D. Raid 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RAID 1+0 (RAID 10) doubles the amount of I/O required from the instance to EBS compared to RAID 0, because you're mirroring all writes to a pair of volumes, limiting how much you can stripe.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

QUESTION 237
In the context of IAM roles for Amazon EC2, which of the following NOT true about delegating permission to make API requests?

A. You cannot create an IAM role.
B. You can have the application retrieve a set of temporary credentials and use them.
C. You can specify the role when you launch your instances.
D. You can define which accounts or AWS services can assume the role.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Amazon designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows: Create an IAM role. Define which accounts or AWS services can assume the role. Define which API actions and resources the application can use after assuming the role. Specify the role when you launch your instances. Have the application retrieve a set of temporary credentials and use them.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

QUESTION 238

In the context of Amazon ElastiCache CLI, which of the following commands can you use to view all ElastiCache instance events for the past 24 hours?

A. elasticache-events --duration 24

B. elasticache-events --duration 1440

C. elasticache-describe-events --duration 24

D. elasticache describe-events --source-type cache-cluster --duration 1440

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In Amazon ElastiCache, the code "aws elasticache describe-events --source-type cache-cluster -- duration 1440" is used to list the cache-cluster events for the past 24 hours (1440 minutes).

http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/ECEvents.Viewing.html

QUESTION 239

In Amazon Cognito what is a silent push notification?

A. It is a push message that is received by your application on a user's device that will not be seen by the user.

B. It is a push message that is received by your application on a user's device that will return the user's geolocation.

C. It is a push message that is received by your application on a user's device that will not be heard by the user.

D. It is a push message that is received by your application on a user's device that will return the user's authentication credentials.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Amazon Cognito uses the Amazon Simple Notification Service (SNS) to send silent push notifications to devices. A silent push notification is a push message that is received by your application on a user's device that will not be seen by the user. http://aws.amazon.com/cognito/faqs/

QUESTION 240

When using Numeric Conditions within IAM, short versions of the available comparators can be used instead of the more verbose versions.

Which of the following is the short version of the Numeric Condition "NumericLessThanEquals"?

A. numlteq

B. numlteql

C. numltequals

D. numeql

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When using Numeric Conditions within IAM, short versions of the available comparators can be used instead of the more verbose versions. For instance, numlteq is the short version of NumericLessThanEquals.

http://awsdocs.s3.amazonaws.com/SQS/2011-10-01/sqs-dg-2011-10-01.pdf

QUESTION 241
AWS has launched T2 instances which come with CPU usage credit. An organization has a requirement which keeps an instance running for 24 hours. However, the organization has high usage only during 11 AM to 12 PM. The organization is planning to use a T2 small instance for this purpose.

If the organization already has multiple instances running since Jan 2012, which of the below mentioned options should the organization implement while launching a T2 instance?

A. The organization must migrate to the EC2-VPC platform first before launching a T2 instance.
B. While launching a T2 instance the organization must create a new AWS account as this account does not have the EC2-VPC platform.
C. Create a VPC and launch a T2 instance as part of one of the subnets of that VPC.
D. While launching a T2 instance the organization must select EC2-VPC as the platform.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC. The AWS account provides two platforms:
EC2-CLASSIC and EC2-VPC, depending on when the user has created his AWS account and which regions he is using. If the user has created the AWS account after 2013-12-04, it supports only EC2-VPC. In this scenario, since the account is before the required date the supported platform will be EC2-CLASSIC. It is required that the organization creates a VPC as the T2 instances can be launched only as a part of VPC.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/vpc-migrate.html

QUESTION 242
How does AWS Data Pipeline execute activities on on-premise resources or AWS resources that you manage?
A. By supplying a Task Runner package that can be installed on your on-premise hosts
B. None of these
C. By supplying a Task Runner file that the resources can access for execution
D. By supplying a Task Runner json script that can be installed on your on-premise hosts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To enable running activities using on-premise resources, AWS Data Pipeline does the following: It supply a Task Runner package that can be installed on your on-premise hosts. This package continuously polls the AWS Data Pipeline service for work to perform. When it's time to run a particular activity on your on-premise resources, it will issue the appropriate command to the Task Runner. https://aws.amazon.com/datapipeline/faqs/

QUESTION 243 Which of following IAM policy elements lets you specify an exception to a list of actions?

A. NotException
B. ExceptionAction
C. Exception
D. NotAction

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The NotAction element lets you specify an exception to a list of actions.
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

QUESTION 244 In AWS IAM, which of the following predefined policy condition keys checks how long ago (in seconds) the MFA-validated security credentials making the request were issued using multi- factor authentication (MFA)?

A. aws:MultiFactorAuthAge
B. aws:MultiFactorAuthLast
C. aws:MFAAge
D. aws:MultiFactorAuthPrevious

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
aws:MultiFactorAuthAge is one of the predefined keys provided by AWS that can be included within a Condition element of an IAM policy. The key allows to check how long ago (in seconds) the MFA-validated security credentials making the request were issued using Multi-Factor Authentication (MFA). http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

QUESTION 245
A user is configuring MySQL RDS with PIOPS. What should be the minimum PIOPS that the user should provision?

A. 1000
B. 200
C. 2000
D. 500

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If a user is trying to enable PIOPS with MySQL RDS, the minimum size of storage should be 100 GB and the minimum PIOPS should be 1000.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.html

QUESTION 246
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 1 only
B. RAID 5 only
C. RAID 5 and RAID 6
D. RAID 0 only

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

QUESTION 247
Once the user has set ElastiCache for an application and it is up and running, which services, does Amazon not provide for the user:

A. The ability for client programs to automatically identify all of the nodes in a cache cluster, and to initiate and maintain connections to all of these nodes
B. Automating common administrative tasks such as failure detection and recovery, and software patching.
C. Providing default Time to Live (TTL) in the AWS Elasticache Redis Implementation for different type of data.

D. Providing detailed monitoring metrics associated with your Cache Nodes, enabling you to diagnose and react to issues very quickly

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon provides failure detection and recovery, and software patching and monitoring tools which is called CloudWatch. In addition it provides also Auto Discovery to automatically identify and initialize all nodes of cache cluster for Amazon ElastiCache. http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/WhatIs.html

QUESTION 248
In the context of AWS Cloud Hardware Security Module(HSM), does your application need to reside in the same VPC as the CloudHSM instance?

A. No, but the server or instance on which your application and the HSM client is running must have network (IP) reachability to the HSM.
B. Yes, always
C. No, but they must reside in the same Availability Zone.
D. No, but it should reside in same Availability Zone as the DB instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Your application does not need to reside in the same VPC as the CloudHSM instance. However, the server or instance on which your application and the HSM client is running must have network (IP) reachability to the HSM. You can establish network connectivity in a variety of ways, including operating your application in the same VPC, with VPC peering, with a VPN connection, or with Direct Connect. https://aws.amazon.com/cloudhsm/faqs/

QUESTION 249
True or False: In Amazon ElastiCache, you can use Cache Security Groups to configure the cache clusters that are part of a VPC.

A. FALSE
B. TRUE
C. True, this is applicable only to cache clusters that are running in an Amazon VPC environment.
D. True, but only when you configure the cache clusters using the Cache Security Groups from the console navigation pane.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon ElastiCache cache security groups are only applicable to cache clusters that are not running in an Amazon Virtual Private Cloud environment (VPC). If you are running in an Amazon Virtual Private Cloud, Cache Security Groups is not available in the console navigation pane. http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/CacheSecurityGroup.html

QUESTION 250
What is the role of the PollForTask action when it is called by a task runner in AWS Data Pipeline?

A. It is used to retrieve the pipeline definition.
B. It is used to report the progress of the task runner to AWS Data Pipeline.
C. It is used to receive a task to perform from AWS Data Pipeline.
D. It is used to inform AWS Data Pipeline of the outcome when the task runner completes a task.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Task runners call PollForTask to receive a task to perform from AWS Data Pipeline. If tasks are ready in the work queue, PollForTask returns a response immediately. If no tasks are available in the queue, PollForTask uses long-polling and holds on to a poll connection for up to 90 seconds, during which time any newly scheduled tasks are handed to the task agent. Your remote worker should not call PollForTask again on the same worker group until it receives a response, and this may take up to 90 seconds. http://docs.aws.amazon.com/datapipeline/latest/APIReference/API_PollForTask.html

QUESTION 251
What is the average queue length recommended by AWS to achieve a lower latency for the 200 PIOPS EBS volume?

A. 5
B. 1
C. 2
D. 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The queue length is the number of pending I/O requests for a device. The optimal average queue length will vary for every customer workload, and this value depends on a particular application's sensitivity to IOPS and latency. If the workload is not delivering enough I/O requests to maintain the optimal average queue length, then the EBS volume might not consistently deliver the IOPS that have been provisioned. However, if the workload maintains an average queue length that is higher than the optimal value, then the per-request I/O latency will increase; in this case, the user should provision more IOPS for his volume. AWS recommends that the user should target an optimal average queue length of 1 for every 200 provisioned IOPS and tune that value based on his application requirements. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-workload-demand.html

QUESTION 252
Who is responsible for modifying the routing tables and networking ACLs in a VPC to ensure that a DB instance is reachable from other instances in the VPC?

A. AWS administrators
B. The owner of the AWS account
C. Amazon
D. The DB engine vendor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You are in charge of configuring the routing tables of your VPC as well as the network ACLs rules needed to make your DB instances accessible from all the instances of your VPC that need to communicate with it.
http://aws.amazon.com/rds/faqs/

QUESTION 253
An organization is planning to host a web application in the AWS VPC. The organization does not want to host a database in the public cloud due to statutory requirements.

How can the organization setup in this scenario?

A. The organization should plan the app server on the public subnet and database in the organization's data center and connect them with the VPN gateway.
B. The organization should plan the app server on the public subnet and use RDS with the private subnet for a secure data operation.
C. The organization should use the public subnet for the app server and use RDS with a storage gateway to access as well as sync the data securely from the local data center.
D. The organization should plan the app server on the public subnet and database in a private subnet so it will not be in the public cloud.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will create a virtual private gateway to route all the traffic of the VPN subnet. If the virtual private gateway is attached with VPC and the user deletes the VPC from the console it will first automatically detach the gateway and only then delete the VPC. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 254
A user is trying to create a PIOPS EBS volume with 4000 IOPS and 100 GB size. AWS does not allow the user to create this volume.

What is the possible root cause for this?

A. PIOPS is supported for EBS higher than 500 GB size
B. The maximum IOPS supported by EBS is 3000
C. The ratio between IOPS and the EBS volume is higher than 30
D. The ratio between IOPS and the EBS volume is lower than 50

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Provisioned IOPS (SSD) volume can range in size from 4 GiB to 16 TiB and you can provision up to 20,000 IOPS per volume. The ratio of IOPS provisioned to the volume size requested should be a maximum of 30; for example, a volume with 3000 IOPS must be at least 100 GB. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_piops

QUESTION 255
A user is planning to host a Highly Available system on the AWS VPC. Which of the below mentioned statements is helpful in this scenario?

A. Create VPC subnets in two separate availability zones and launch instances in different subnets.
B. Create VPC with only one public subnet and launch instances in different AZs using that subnet.
C. Create two VPCs in two separate zones and setup failover with ELB such that if one VPC fails it will divert traffic to another VPC.
D. Create VPC with only one private subnet and launch instances in different AZs using that subnet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. The VPC is always specific to a region. The user can create a VPC which can span multiple Availability Zones by adding one or more subnets in each Availability Zone. Each subnet must reside entirely within one Availability Zone and cannot span across zones.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPCSubnet

QUESTION 256
A user is creating a PIOPS volume. What is the maximum ratio the user should configure between PIOPS and the volume size?

A. 5
B. 10C. 20
D. 30

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Provisioned IOPS volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput. A provisioned IOPS volume can range in size from 10 GB to 1 TB and the user can provision up to 4000 IOPS per volume.
The ratio of IOPS provisioned to the volume size requested can be a maximum of 30; for example, a volume with 3000 IOPS must be at least 100 GB.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

QUESTION 257 What is a possible reason you would need to edit claims issued in a SAML token?

A. The NameIdentifier claim cannot be the same as the username stored in AD.
B. Authentication fails consistently.
C. The NameIdentifier claim cannot be the same as the claim URI.
D. The NameIdentifier claim must be the same as the username stored in AD.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The two reasons you would need to edit claims issued in a SAML token are:
The NameIdentifier claim cannot be the same as the username stored in AD, and The app requires a different set of claim URIs.
https://azure.microsoft.com/en-us/documentation/articles/active-directory-saml-claims-customization/

QUESTION 258
A government client needs you to set up secure cryptographic key storage for some of their extremely confidential data. You decide that the AWS CloudHSM is the best service for this. However, there seem to be a few pre-requisites before this can happen, one of those being a security group that has certain ports open.

Which of the following is correct in regards to those security groups?

A. A security group that has no ports open to your network.
B. A security group that has only port 3389 (for RDP) open to your network.
C. A security group that has only port 22 (for SSH) open to your network.
D. A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudHSM provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud.
AWS CloudHSM requires the following environment before an HSM appliance can be provisioned. A virtual private cloud (VPC) in the region where you want the AWS CloudHSM service. One private subnet (a subnet with no Internet gateway) in the VPC. The HSM appliance is provisioned into this subnet.
One public subnet (a subnet with an Internet gateway attached). The control instances are attached to this subnet.
An AWS Identity and Access Management (IAM) role that delegates access to your AWS resources to AWS CloudHSM.
An EC2 instance, in the same VPC as the HSM appliance, that has the SafeNet client software installed. This instance is referred to as the control instance and is used to connect to and manage the HSM appliance. A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network. This security group is attached to your control instances so you can access them remotely.

QUESTION 259 What is the network performance offered by the c4.8xlarge instance in Amazon EC2?

A. Very High but variable
B. 20 Gigabit
C. 5 Gigabit
D. 10 Gigabit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Networking performance offered by the c4.8xlarge instance is 10 Gigabit. http://aws.amazon.com/ec2/instance-types/

QUESTION 260

An organization is setting up a web application with the JEE stack. The application uses the JBoss app server and MySQL DB. The application has a logging module which logs all the activities whenever a business function of the JEE application is called. The logging activity takes some time due to the large size of the log file.

If the application wants to setup a scalable infrastructure which of the below mentioned options will help achieve this setup?

A. Host the log files on EBS with PIOPS which will have higher I/O.
B. Host logging and the app server on separate servers such that they are both in the same zone.
C. Host logging and the app server on the same instance so that the network latency will be shorter.
D. Create a separate module for logging and using SQS compartmentalize the module such that all calls to logging are asynchronous.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The organization can always launch multiple EC2 instances in the same region across multiple AZs for HA and DR. The AWS architecture practice recommends compartmentalizing the functionality such that they can both run in parallel without affecting the performance of the main application. In this scenario logging takes a longer time due to the large size of the log file. Thus, it is recommended that the organization should separate them out and make separate modules and make asynchronous calls among them. This way the application can scale as per the requirement and the performance will not bear the impact of logging. http://www.awsarchitectureblog.com/2014/03/aws-and-compartmentalization.html

QUESTION 261

You're trying to delete an SSL certificate from the IAM certificate store, and you're getting the message "Certificate: <certificate-id> is being used by CloudFront." Which

of the following statements is probably the reason why you are getting this error?

A. Before you can delete an SSL certificate you need to set up https on your server.
B. Before you can delete an SSL certificate, you need to set up the appropriate access level in IAM
C. Before you can delete an SSL certificate, you need to either rotate SSL certificates or revert from using a custom SSL certificate to using the default CloudFront certificate.
D. You can't delete SSL certificates. You need to request it from AWS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudFront is a web service that speeds up distribution of your static and dynamic web content, for example, .html, .css,.php, and image files, to end users. Every CloudFront web distribution must be associated either with the default CloudFront certificate or with a custom SSL certificate. Before you can delete an SSL certificate, you need to either rotate SSL certificates (replace the current custom SSL certificate with another custom SSL certificate) or revert from using a custom SSL certificate to using the default CloudFront certificate. http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Troubleshooting.html

QUESTION 262

A user has set the IAM policy where it denies all requests if a request is not from IP 10.10.10.1/32. The other policy says allow all requests between 5 PM to 7 PM.

What will happen when a user is requesting access from IP 55.109.10.12/32 at 6 PM?

A. It will deny access
B. It is not possible to set a policy based on the time or IP
C. IAM will throw an error for policy conflict
D. It will allow access

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When a request is made, the AWS IAM policy decides whether a given request should be allowed or denied. The evaluation logic follows these rules:
By default, all requests are denied. (In general, requests made using the account credentials for resources in the account are always allowed.) An explicit allow policy overrides this default. An explicit deny policy overrides any allows.
In this case since there are explicit deny and explicit allow statements. Thus, the request will be denied since deny overrides allow.
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

QUESTION 263 Do you need to use Amazon Cognito to use the Amazon Mobile Analytics service?

A. No. However, it is recommend by AWS to use Amazon Cognito for security best practices.
B. Yes. You need to use it only if you have IAM root access.
C. No. You cannot use it at all, and you need to use AWS IAM accounts.
D. Yes. It is recommended by AWS to use Amazon Cognito to use Amazon Mobile Analytics service.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can initialize Amazon Mobile Analytics using AWS IAM accounts. AWS recommend using Amazon Cognito for security best practices. http://aws.amazon.com/mobileanalytics/faqs/

QUESTION 264 Which of the following AWS services can be used to define alarms to trigger on a certain activity, such as activity success, failure, or delay in AWS Data Pipeline?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS Data Pipeline, you can define Amazon SNS alarms to trigger on activities such as success, failure, or delay by creating an alarm object and referencing it in the onFail, onSuccess, or onLate slots of the activity object.
https://aws.amazon.com/datapipeline/faqs/

QUESTION 265 You want to use Amazon Redshift and you are planning to deploy dw1.8xlarge nodes. What is the minimum amount of nodes that you need to deploy with this kind of configuration?

A. 1
B. 4
C. 3
D. 2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For a single-node configuration in Amazon Redshift, the only option available is the smallest of the two options. The 8XL extra-large nodes are only available in a multi-node configuration.
http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-clusters.html

QUESTION 266

Mike is appointed as Cloud Consultant in ABC.com. ABC has the following VPCs set- up in the US East Region:
A VPC with CIDR block 10.10.0.0/16, a subnet in that VPC with CIDR block 10.10.1.0/24 A VPC with CIDR block 10.40.0.0/16, a subnet in that VPC with CIDR block 10.40.1.0/24 ABC.com is trying to establish network connection between two subnets, a subnet with CIDR block 10.10.1.0/24 and another subnet with CIDR block 10.40.1.0/24.

Which one of the following solutions should Mike recommend to ABC.com?

A. Create 2 Virtual Private Gateways and configure one with each VPC.
B. Create 2 Internet Gateways, and attach one to each VPC.
C. Create a VPC Peering connection between both VPCs.
D. Create one EC2 instance in each subnet, assign Elastic IPs to both instances, and configure a set up Site-to-Site VPN connection between both EC2 instances.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. EC2 instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

QUESTION 267
Can Provisioned IOPS be used on RDS instances launched in a VPC?

A. Yes, they can be used only with Oracle based instances.
B. Yes, they can be used for all RDS instances.
C. No
D. Yes, they can be used only with MySQL based instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The basic building block of Amazon RDS is the DB instance. DB instance storage comes in three types:
Magnetic, General Purpose (SSD), and Provisioned IOPS (SSD). When you buy a server, you get CPU, memory, storage, and IOPS, all bundled together. With Amazon RDS, these are split apart so that you can scale them independently. So, for example, if you need more CPU, less IOPS, or more storage, you can easily allocate them.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/RDSFAQ.PIOPS.html

QUESTION 268
To get started using AWS Direct Connect, in which of the following steps do you configure Border Gateway Protocol (BGP)?

A. Complete the Cross Connect
B. Configure Redundant Connections with AWS Direct Connect
C. Create a Virtual Interface
D. Download Router Configuration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: In AWS Direct Connect, your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication, and you need to provide a private Autonomous System Number (ASN) for that to connect to Amazon Virtual Private Cloud (VPC). To connect to public AWS products such as Amazon EC2 and Amazon S3, you will also need to provide a public ASN that you own (preferred) or a private ASN. You have to configure BGP in the Create a Virtual Interface step. http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#createvirtualinterface

QUESTION 269
Which of the following components of AWS Data Pipeline polls for tasks and then performs those tasks?

A. Pipeline Definition
B. Task Runner
C. Amazon Elastic MapReduce (EMR)
D. AWS Direct Connect

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Task Runner polls for tasks and then performs those tasks.
http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html

QUESTION 270
A user is hosting a public website on AWS. The user wants to have the database and the app server on the AWS VPC. The user wants to setup a database that can connect to the Internet for any patch upgrade but cannot receive any request from the internet. How can the user set this up?

A. Setup DB in a private subnet with the security group allowing only outbound traffic.
B. Setup DB in a public subnet with the security group allowing only inbound data.
C. Setup DB in a local data center and use a private gateway to connect the application with DB.
D. Setup DB in a private subnet which is connected to the internet via NAT for outbound.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. AWS provides two features that the user can use to increase security in VPC: security groups and network ACLs. When the user wants to setup both the DB and App on VPC, the user should make one public and one private subnet. The DB should be hosted in a private subnet and instances in that subnet cannot reach the internet. The user can allow an instance in his VPC to initiate outbound connections to the internet but prevent unsolicited inbound connections from the internet by using a Network Address Translation (NAT) instance. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 271
An organization is setting up their website on AWS. The organization is working on various security measures to be performed on the AWS EC2 instances.

Which of the below mentioned security mechanisms will not help the organization to avoid future data leaks and identify security weaknesses?

A. Run penetration testing on AWS with prior approval from Amazon.
B. Perform SQL injection for application testing.
C. Perform a Code Check for any memory leaks.
D. Perform a hardening test on the AWS instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS security follows the shared security model where the user is as much responsible as Amazon. Since Amazon is a public cloud it is bound to be targeted by hackers. If an organization is planning to host their application on AWS EC2, they should perform the below mentioned security checks as a measure to find any security weakness/data leaks:
Perform penetration testing as performed by attackers to find any vulnerability. The organization must take an approval from AWS before performing penetration testing Perform hardening testing to find if there are any unnecessary ports open Perform SQL injection to find any DB security issues
The code memory checks are generally useful when the organization wants to improve the application performance. http://aws.amazon.com/security/penetration-testing/

QUESTION 272 In Amazon ElastiCache, the
default cache port is:

A. for Memcached 11210 and for Redis 6380. B.
for Memcached 11211 and for Redis 6380. C.
for Memcached 11210 and for Redis 6379.
D. for Memcached 11211 and for Redis 6379.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon ElastiCache, you can specify a new port number for your cache cluster, which by default is 11211 for Memcached and 6379 for Redis.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/GettingStarted.AuthorizeAccess.html

QUESTION 273
A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. The NAT instance ID is i-a12345.

Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?

A. Destination: 20.0.0.0/0 and Target: 80
B. Destination: 20.0.0.0/0 and Target: i-a12345
C. Destination: 20.0.0.0/24 and Target: i-a12345
D. Destination: 0.0.0.0/0 and Target: i-a12345

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create two route tables and attach to the subnets. The main route table will have the entry "Destination: 0.0.0.0/0 and Target: i-a12345", which allows all the instances in the private subnet to connect to the internet using NAT. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 274
Which of the following cannot be used to manage Amazon ElastiCache and perform administrative tasks?

A. AWS software development kits (SDKs)
B. Amazon S3
C. ElastiCache command line interface (CLI)
D. AWS CloudWatch

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudWatch is a monitoring tool and doesn't give users access to manage Amazon ElastiCache. http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/WhatIs.Managing.html

QUESTION 275 Which of the following statements is correct about AWS
Direct Connect?

A. Connections to AWS Direct Connect require double clad fiber for 1 gigabit Ethernet with Auto Negotiation enabled for the port.
B. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with.
C. AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 50 gigabit Ethernet cable.
D. To use AWS Direct Connect, your network must be collocated with a new AWS Direct Connect location.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. To use AWS Direct Connect, your network is collocated with an existing AWS Direct Connect location. Connections to AWS Direct Connect require single mode fiber, 1000BASELX (1310nm) for 1 gigabit Ethernet, or 10GBASE-LR (1310nm) for 10 gigabit Ethernet. Auto Negotiation for the port must be disabled.
http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION 276
Which of the following statements is correct about the number of security groups and rules applicable for an EC2-Classic instance and an EC2-VPC network interface?

A. In EC2-Classic, you can associate an instance with up to 5 security groups and add up to 50 rules to a security group. In EC2-VPC, you can associate a network interface with up to 500 security groups and add up to 100 rules to asecurity group.
B. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 50 rules to a security group. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 100 rules to asecurity group.
C. In EC2-Classic, you can associate an instance with up to 5 security groups and add up to 100 rules to a security group. In EC2-VPC, you can associate a network interface with up to 500 security groups and add up to 50 rules to asecurity group.
D. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 100 rules to a security group. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 50 rules to a

security group.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 100 rules to a security group. If you're using EC2-VPC, you must use security groups created specifically for your VPC. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 50 rules to a security group.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 277 Is there any way to own a direct connection to
Amazon Web Services?

A. No, AWS only allows access from the public Internet.
B. No, you can create an encrypted tunnel to VPC, but you cannot own the connection.C. Yes, you can via Amazon Dedicated Connection
D. Yes, you can via AWS Direct Connect.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to the AWS cloud (for example, to Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3)) and to Amazon Virtual Private Cloud (Amazon VPC), bypassing Internet service providers in your network path. http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION 278 Identify a true statement about the
statement ID (Sid) in IAM.

A. You cannot expose the Sid in the IAM API.
B. You cannot use a Sid value as a sub-ID for a policy document's ID for services provided by SQS and SNS.
C. You can expose the Sid in the IAM API.

D. You cannot assign a Sid value to each statement in a statement array.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Sid (statement ID) is an optional identifier that you provide for the policy statement. You can assign a Sid a value to each statement in a statement array. In IAM, the Sid is not exposed in the IAM API. You can't retrieve a particular statement based on this ID. http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html#Sid

QUESTION 279 In Amazon ElastiCache, which of the following statements is correct?

A. When you launch an ElastiCache cluster into an Amazon VPC private subnet, every cache node is assigned a public IP address within that subnet.
B. You cannot use ElastiCache in a VPC that is configured for dedicated instance tenancy.
C. If your AWS account supports only the EC2-VPC platform, ElastiCache will never launch your cluster in a VPC.
D. ElastiCache is not fully integrated with Amazon Virtual Private Cloud (VPC).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The VPC must allow non-dedicated EC2 instances. You cannot use ElastiCache in a VPC that is configured for dedicated instance tenancy.
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/AmazonVPC.EC.html

QUESTION 280
An organization has setup RDS with VPC. The organization wants RDS to be accessible from the internet. Which of the below mentioned configurations is not required in this scenario?

A. The organization must enable the parameter in the console which makes the RDS instance publicly accessible. B.
The organization must allow access from the internet in the RDS VPC security group,
C. The organization must setup RDS with the subnet group which has an external IP.
D. The organization must enable the VPC attributes DNS hostnames and DNS resolution.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources, such as RDS into a virtual network that the user has defined. Subnets are segments of a VPC's IP address range that the user can designate to a group of VPC resources based on security and operational needs. A DB subnet group is a collection of subnets (generally private) that the user can create in a VPC and which the user assigns to the RDS DB instances. A DB subnet group allows the user to specify a particular VPC when creating DB instances. If the RDS instance is required to be accessible from the internet:
The organization must setup that the RDS instance is enabled with the VPC attributes, DNS hostnames and DNS resolution.
The organization must enable the parameter in the console which makes the RDS instance publicly accessible.
The organization must allow access from the internet in the RDS VPC security group.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.html

QUESTION 281
An organization, which has the AWS account ID as 999988887777, has created 50 IAM users. All the users are added to the same group ABC.
If the organization has enabled that each IAM user can login with the AWS console, which AWS login URL will the IAM users use??

A. https://999988887777.aws.amazon.com/ABC/
B. https://signin.aws.amazon.com/ABC/
C. https://ABC.signin.aws.amazon.com/999988887777/console/
D. https://999988887777.signin.aws.amazon.com/console/

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Identity and Access Management is a web service which allows organizations to manage users and user permissions for various AWS services. Once the organization has created the IAM users, they will have a separate AWS console URL to login to the AWS console. The console login URL for the IAM user will be https:// AWS_Account_ID.signin.aws.amazon.com/console/. It uses only the AWS account ID and does not depend on the group or user ID.
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccountAlias.html

QUESTION 282 Can you configure multiple Load Balancers with a single Auto Scaling group?

A. No
B. Yes, you can but only if it is configured with Amazon Redshift.
C. Yes, you can provide the ELB is configured with Amazon AppStream.
D. Yes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Yes, you can configure more than one load balancer with an autoscaling group. Auto Scaling integrates with Elastic Load Balancing to enable you to attach one or more load balancers to an existing Auto Scaling group. After you attach the load balancer, it automatically registers the instances in the group and distributes incoming traffic across the instances. http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION 283
An Auto Scaling group is running at the desired capacity of 5 instances and receives a trigger from the Cloudwatch Alarm to increase the capacity by 1. The cool down period is 5 minutes. Cloudwatch sends another trigger after 2 minutes to decrease the desired capacity by 1.

What will be the count of instances at the end of 4 minutes?

A. 4
B. 5
C. 6
D. 7

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The cool down period is the time difference between the end of one scaling activity (can be start or terminate) and the start of another one (can be start or terminate). During the cool down period, Auto Scaling does not allow the desired capacity of the Auto Scaling group to be changed by any other CloudWatch alarm. Thus, in this case the trigger from the second alarm will have no effect.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html#healthcheck

QUESTION 284 Which of the following is NOT a true statement about Auto Scaling?

A. Auto Scaling can launch instances in different Azs.
B. Auto Scaling can work with CloudWatch.
C. Auto Scaling can launch an instance at a specific time.
D. Auto Scaling can launch instances in different regions.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling provides an option to scale up and scale down based on certain conditions or triggers from Cloudwatch. A user can configure such that Auto Scaling launches instances across Azs, but it cannot span across regions.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-dg.pdf

QUESTION 285
A user wants to configure AutoScaling which scales up when the CPU utilization is above 70% and scales down when the CPU utilization is below 30%.

How can the user configure AutoScaling for the above mentioned condition?

A. Configure ELB to notify AutoScaling on load increase or decrease
B. Use AutoScaling with a schedule
C. Use AutoScaling by manually modifying the desired capacity during a condition
D. Use dynamic AutoScaling with a policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: The user can configure the AutoScaling group to automatically scale up and then scale down based on the specified conditions. To configure this, the user must setup policies which will get triggered by the CloudWatch alarms.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-scale-based-on-demand.html

QUESTION 286 Can a user configure a custom health check
with Auto Scaling?

A. Yes, but the configured data will not be saved to Auto Scaling.
B. No, only an ELB health check can be configured with Auto Scaling.
C. Yes
D. No

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Auto Scaling can determine the health status of an instance using custom health checks. If you have custom health checks, you can send the information from your health checks to Auto Scaling so that Auto Scaling can use this information. For example, if you determine that an instance is not functioning as expected, you can set the health status of the instance to Unhealthy. The next time that Auto Scaling performs a health check on the instance, it will determine that the instance is unhealthy and then launch a replacement instance. http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/healthcheck.html

QUESTION 287
You have setup an Auto Scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first scaling activity request for the Auto Scaling group is to launch two instances. It receives the activity question at time "t", and the first instance is launched at t+3 minutes, while the second instance is launched at t+4 minutes.

How many minutes after time "t" will Auto Scaling accept another scaling activity request?

A. 11 minutes
B. 10 minutesC. 7 minutes
D. 14 minutes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION 288
You have just added a new instance to your Auto Scaling group, which receives ELB health checks. An ELB heath check says the new instance's state is out of Service.

What does Auto Scaling do in this particular scenario?

A. It replaces the instance with a healthy one
B. It stops the instance
C. It marks an instance as unhealthy
D. It terminates the instance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you have attached a load balancer to your Auto Scaling group, you can have Auto Scaling include the results of Elastic Load Balancing health checks when it determines the health status of an instance. After you add ELB health checks, Auto Scaling will mark an instance as unhealthy if Elastic Load Balancing reports the instance state as Out of Service. Frequently, an Auto Scaling instance that has just come into service needs to warm up before it can pass the Auto Scaling health check. Auto Scaling waits until the health check grace period ends before checking the health status of the instance. While the EC2 status checks and ELB health checks can complete before the health check grace period expires, Auto Scaling does not act on them until the health check grace period expires. To provide ample warm-up time for your instances, ensure that the health check grace period covers the expected startup time for your application.
http://docs.aws.amazon.com/autoscaling/latest/userguide/healthcheck.html

QUESTION 289
A sys admin is maintaining an application on AWS. The application is installed on EC2 and user has configured ELB and Auto Scaling. Considering future load increase, the user is planning to launch new servers proactively so that they get registered with ELB.

How can the user add these instances with Auto Scaling?

A. Decrease the minimum limit of the Auto Scaling group
B. Increase the maximum limit of the Auto Scaling group
C. Launch an instance manually and register it with ELB on the fly
D. Increase the desired capacity of the Auto Scaling group

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user can increase the desired capacity of the Auto Scaling group and Auto Scaling will launch a new instance as per the new capacity. The newly launched instances will be registered with ELB if Auto Scaling group is configured with ELB. If the user decreases the minimum size the instances will be removed from Auto Scaling. Increasing the maximum size will not add instances but only set the maximum instance cap.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-manual-scaling.html

QUESTION 290
You have set up Auto Scaling to automatically scale in. Consequently, you must decide which instances Auto Scaling should end first.

What should you use to configure this?

A. An Elastic Load Balancer
B. A termination policy
C. An IAM role
D. Another scaling group

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you instruct Auto Scaling to automatically scale in, you must decide which instances Auto Scaling should terminate first. This can be configured through the use of a termination policy.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingBehavior.InstanceTermination.html

QUESTION 291 Which of the following commands accepts binary data as parameters?

A. --user-data
B. –cipher text-key
C. --aws-customer-key
D. --describe-instances-user

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For commands that take binary data as a parameter, specify that the data is binary content by using the fileb:// prefix.
Commands that accept binary data include: aws ec2 run-instances --user-data parameter.
aws s3api put-object --sse-customer-key parameter. aws kms decrypt --ciphertext-blob parameter. http://docs.aws.amazon.com/cli/latest/userguide/aws-cli.pdf

QUESTION 292
To scale out the AWS resources using manual AutoScaling, which of the below mentioned parameters should the user change?

A. Current capacity
B. Desired capacity
C. Preferred capacity
D. Maximum capacity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Manual Scaling as part of Auto Scaling allows the user to change the capacity of Auto Scaling group. The user can add / remove EC2 instances on the fly. To execute manual scaling, the user should modify the desired capacity. AutoScaling will adjust instances as per the requirements.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-manual-scaling.html

QUESTION 293
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 and CloudWatch?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
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. http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/healthcheck.html

QUESTION 294 Identify a benefit of using Auto Scaling for your application.

A. Your application gains better fault tolerance.
B. Your application optimizes only logistics and operations.
C. Your application receives latency requirements in every region.
D. You acquire clarity on prototypes in your application.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you use Auto Scaling, your applications gain better fault tolerance. Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. You can also configure Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Auto Scaling can launch instances in another one to compensate. http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/how-as-works.html

QUESTION 295
A user has suspended the scaling process on the Auto Scaling group. A scaling activity to increase the instance count was already in progress.

What effect will the suspension have on that activity?

A. No effect. The scaling activity continues
B. Pauses the instance launch and launches it only after Auto Scaling is resumed
C. Terminates the instance
D. Stops the instance temporary

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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. When this process is suspended, Auto Scaling creates no new scaling activities for that group. Scaling activities that were already in progress before the group was suspended continue until completed.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

QUESTION 296 Does Autoscaling automatically assign tags to resources?

A. No, not unless they are configured via API.
B. Yes, it does.
C. Yes, by default.
D. No, it does not.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Tags don't have any semantic meaning to Amazon EC2 and are interpreted strictly as a string of characters.
Tags are assigned automatically to the instances created by an Auto Scaling group. Auto Scaling adds a tag to the instance with a key of aws: autoscaling:groupName and a value of the name of the Auto Scaling group.
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Using_Tags.html

QUESTION 297 If you have a running instance using an Amazon EBS boot partition, you can call the _______ API to release the compute resources but preserve the data on the boot partition.

A. Stop Instances
B. Terminate Instances
C. AMI Instance
D. Ping Instance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If you have a running instance using an Amazon EBS boot partition, you can also call the Stop Instances API to release the compute resources but preserve the data on the boot partition.
https://aws.amazon.com/ec2/faqs/#How_quickly_will_systems_be_running

QUESTION 298 Which EC2 functionality allows the user to place the Cluster Compute instances in clusters?

A. Cluster group
B. Cluster security group
C. GPU units
D. Cluster placement group

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon EC2 cluster placement group functionality allows users to group cluster compute instances in clusters. https://aws.amazon.com/ec2/faqs/

QUESTION 299
A user has launched a dedicated EBS backed instance with EC2. You are curious where the EBS volume for this instance will be created.

Which statement is correct about the EBS volume's creation?

A. The EBS volume will not be created on the same tenant hardware assigned to the dedicated instance
B. AWS does not allow a dedicated EBS backed instance launch
C. The EBS volume will be created on the same tenant hardware assigned to the dedicated instanceD. The user can specify where the EBS will be created

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The dedicated instances are Amazon EC2 instances that run in a Virtual Private Cloud (VPC) on hardware that is dedicated to a single customer. When a user launches an Amazon EBS-backed dedicated instance, the EBS volume does not run on single-tenant hardware. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html

QUESTION 300
Which system is used by Amazon Machine Images paravirtual (PV) virtualization during the boot process?

A. PV-BOOT
B. PV-AMI
C. PV-WORM
D. PV-GRUB

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon Machine Images that use paravirtual (PV) virtualization use a system called PV-GRUB during the boot process. PV-GRUB is a paravirtual boot loader that runs a patched version of GNU GRUB 0.97. When you start an instance, PV-GRUB starts the boot process and then chain loads the kernel specified by your image's menu.lst file.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/UserProvidedKernels.html

QUESTION 301
You have written a CloudFormation template that creates 1 Elastic Load Balancer fronting 2 EC2 Instances.

Which section of the template should you edit so that the DNS of the load balancer is returned upon creation of the stack?

A. Parameters
B. Outputs
C. Mappings
D. Resources

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can use AWS CloudFormation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application.
In the following example, the output named BackupLoadBalancerDNSName returns the DNS name for the resource with the logical ID BackupLoadBalancer only when the CreateProdResources condition is true. (The second output shows how to specify multiple outputs.) "Outputs" : { "BackupLoadBalancerDNSName" : {
"Description": "The DNSName of the backup load balancer", "Value" : { "Fn::GetAtt" : ["BackupLoadBalancer", "DNSName"]}, "Condition" : "CreateProdResources"
},
"InstanceID" : {
"Description": "The Instance ID", "Value" : { "Ref" : "EC2Instance" }
}
}
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html

QUESTION 302
In CloudFormation, if you want to map an Amazon Elastic Block Store to an Amazon EC2 instance, _________.

A. you reference the logical IDs to associate the block stores with the instance
B. you reference the physical IDs of the instance along with the resource type
C. you reference the instance IDs of the block store along with the resource propertiesD. you reference the physical IDs of both the block stores and the instance

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, if you want to map an Amazon Elastic Block Store to an Amazon EC2 instance, you reference the logical IDs to associate the block stores with the instance.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-resources.html

QUESTION 303
An organization hosts an app on EC2 instances which multiple developers need access to in order to perform updates.
The organization plans to implement some security best practices related to instance access.

Which one of the following recommendations will not help improve its security in this way?

A. Disable the password based login for all the users. All the users should use their own keys to connect with the instance securely.
B. Create an IAM policy allowing only IAM users to connect to the EC2 instances with their own SSH key.
C. Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.
D. Apply the latest patch of OS and always keep it updated.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Since AWS is a public cloud any application hosted on EC2 is prone to hacker attacks. It becomes extremely important for a user to setup a proper security mechanism on the EC2 instances. A few of the security measures are listed below: ▪ Always keep the OS updated with the latest patch
▪ Always create separate users with in OS if they need to connect with the EC2 instances, create their keys and disable their password
▪ Create a procedure using which the admin can revoke the access of the user when the business work on the EC2 instance is completed. . Lock down unnecessary ports
▪ Audit any proprietary applications that the user may be running on the EC2 instance. Provide temporary escalated privileges, such as sudo for users who need to perform occasional privileged tasks
IAM is useful when users are required to work with AWS resources and actions, such as launching an instance. It is not useful in this case because it does not manage who can connect via RDP or SSH with an instance.
http://aws.amazon.com/articles/1233/

QUESTION 304
A user has configured two security groups which allow traffic as given below: 1: SecGrp1:
Inbound on port 80 for 0.0.0.0/0 Inbound on port 22 for 0.0.0.0/0 2: SecGrp2:
Inbound on port 22 for 10.10.10.1/32
If both the security groups are associated with the same instance, which of the below mentioned statements is true?

A. It is not possible to have more than one security group assigned to a single instance
B. It is not possible to create the security group with conflicting rules. AWS will reject the request
C. It allows inbound traffic for everyone on both ports 22 and 80
D. It allows inbound traffic on port 22 for IP 10.10.10.1 and for everyone else on port 80

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user can attach more than one security group to a single EC2 instance. In this case, the rules from each security group are effectively aggregated to create one set of rules. AWS uses this set of rules to determine whether to allow access or not. Thus, here the rule for port 22 with IP 10.10.10.1/32 will merge with IP 0.0.0.0/0 and open ports 22 and 80 for all. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 305
You have a website which requires international presence and consequently you have set it up as follows.
It is hosted on 30 EC2 instances.
It is on in 15 regions around the globe. Each region has 2 instances.
All the instances are a public hosted zone.

Which of the following is the best way to configure your site to maintain availability with minimum downtime if one of the 15 regions was to lose network connectivity for an extended period? (Choose 2 answers)

A. Create a Route 53 Latency Based Routing Record set that resolves to an Elastic Load Balancer in each region and has the Evaluate Target Health flag set to true.
B. Create a Route 53 failover routing policy and configure an active-passive failover.
C. Create a Route 53 Failover Routing Policy and assign each resource record set a unique identifier and a relative weight.
D. Create a Route 53 Geolocation Routing Policy that resolves to an Elastic Load Balancer in each region and has the Evaluate Target Health flag set to false.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation: It is best to use the latency routing policy when you have resources in multiple Amazon EC2 data centers that perform the same function and you want Amazon Route 53 to respond to DNS queries with the resources that provide the best latency. You could also use the failover routing policy (for public hosted zones only) when you want to configure an active-passive failover, in which one resource takes all traffic when it's available and the other resource takes all traffic when the first resource isn't available. http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency

QUESTION 306 A user is accessing an EC2 instance on the SSH port for
IP 10.20.30.40/32.

Which one is a secure way to configure that the instance can be accessed only from this IP?

A. In the security group, open port 22 for IP 10.20.30.40
B. In the security group, open port 22 for IP 10.20.30.0
C. In the security group, open port 22 for IP 10.20.30.40/32
D. In the security group, open port 22 for IP 10.20.30.40/0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS EC2, while configuring a security group, the user needs to specify the IP address in CIDR notation. The CIDR IP range 10.20.30.40/32 says it is for a single IP 10.20.30.40. If the user specifies the IP as 10.20.30.40 only, the security group will not accept and ask for it in a CIDR format. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

QUESTION 307
While assigning a tag to an instance, which of the below mentioned options is not a valid tag key/value pair?

A. Key : "aws" Value:"aws"
B. Key: "aws:name" Value: "instanceAnswer: Aws"
C. Key: "Name :aws" Value: "instanceAnswer: Aws"
D. Key : "nameAnswer: Aws" Value:"aws:instance"

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Services, to help manage EC2 instances as well their usage in a better way, the user can tag the instances. The tags are metadata assigned by the user which consists of a key and value. The tag key cannot have a prefix as "aws:", although it can have only "aws". http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

QUESTION 308 Will you be able to access EC2 snapshots using the regular
Amazon S3 APIs?

A. Yes, you will be able to access using S3 APIs if you have chosen the snapshot to be stored in S3.
B. No, snapshots are only available through the Amazon EBS APIs.
C. Yes, you will be able to access them using S3 APIs as all snapshots are stored in S3.

D. No, snapshots are only available through the Amazon EC2 APIs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
No, snapshots are only available through the Amazon EC2 APIs.
https://aws.amazon.com/ec2/faqs/

QUESTION 309
A user has created an AWS AMI. The user wants the AMI to be available only to his friend and not anyone else. How can the user manage this?

A. Share the AMI with the community and setup the approval workflow before anyone launches it.
B. It is not possible to share the AMI with the selected user.
C. Share the AMI with a friend's AWS account ID.
D. Share the AMI with a friend's AWS login ID.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon Web Services, if a user has created an AMI and wants to share with his friends and colleagues he can share the AMI with their AWS account ID. Once the AMI is shared the other user can access it from the community AMIs under private AMIs options. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html

QUESTION 310 A user is planning to launch multiple EC2 instance same as current running instance.

Which of the below mentioned parameters is not copied by Amazon EC2 in the launch wizard when the user has selected the option "Launch more like this"?

A. Termination protection
B. Tenancy setting
C. Storage
D. Shutdown behavior

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon EC2 console provides a "Launch more like this" wizard option that enables the user to use a current instance as a template for launching other instances. This option automatically populates the Amazon EC2 launch wizard with certain configuration details from the selected instance.
The following configuration details are copied from the selected instance into the launch wizard: AMI ID
Instance type
Availability Zone, or the VPC and subnet in which the selected instance is located Public IPv4 address. If the selected instance currently has a public IPv4 address, the new instance receives a public IPv4 address - regardless of the selected instance's default public IPv4 address setting.
For more information about public IPv4 addresses, see Public IPv4 Addresses and External DNS Hostnames.
Placement group, if applicable
IAM role associated with the instance, if applicable Shutdown behavior setting (stop or terminate) Termination protection setting (true or false)
CloudWatch monitoring (enabled or disabled) Amazon EBS-optimization setting (true or false)
Tenancy setting, if launching into a VPC (shared or dedicated) Kernel ID and RAM disk ID, if applicable User data, if specified
Tags associated with the instance, if applicable Security groups associated with the instance
The following configuration details are not copied from your selected instance; instead, the wizard applies their default settings or behavior:

(VPC only) Number of network interfaces: The default is one network interface, which is the primary network interface (eth0).
Storage: The default storage configuration is determined by the AMI and the instance type.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html

QUESTION 311
A user has launched an EBS optimized instance with EC2. Which of the below mentioned options is the correct statement?

A. It provides additional dedicated capacity for EBS IO
B. The attached EBS will have greater storage capacity
C. The user will have a PIOPS based EBS volume
D. It will be launched on dedicated hardware in VPC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An Amazon EBS-optimized instance uses an optimized configuration stack and provides additional, dedicated capacity for the Amazon EBS I/O. This optimization provides the best performance for the user's Amazon EBS volumes by minimizing contention between the Amazon EBS I/O and other traffic from the user's instance. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html

QUESTION 312 Which status represents a failure state in AWS CloudFormation?

A. ROLLBACK_IN_PROGRESS
B. DELETE_IN_PROGRESS
C. UPDATE_COMPLETE_CLEANUP_IN_PROGRESS
D. REVIEW_IN_PROGRESS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ROLLBACK_IN_PROGRESS means an ongoing removal of one or more stacks after a failed stack creation or after an explicitly canceled stack creation. DELETE_IN_PROGRESS means an ongoing removal of one or more stacks.
REVIEW_IN_PROGRESS means an ongoing creation of one or more stacks with an expected StackId but without any templates or resources.
UPDATE_COMPLETE_CLEANUP_IN_PROGRESS means an ongoing removal of old resources for one or more stacks after a successful stack update.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-describing-stacks.html

QUESTION 313 You are playing around with setting up stacks using JSON templates in CloudFormation to try and understand them a little better. You have set up about 5 or 6 but now start to wonder if you are being charged for these stacks.

What is AWS's billing policy regarding stack resources?

A. You are not charged for the stack resources if they are not taking any traffic.
B. You are charged for the stack resources for the time they were operating (but not if you deleted the stack within 30 minutes)
C. You are charged for the stack resources for the time they were operating (but not if you deleted the stack within 60 minutes)D. You are charged for the stack resources for the time they were operating (even if you deleted the stack right away)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A stack is a collection of AWS resources that you can manage as a single unit. In other words, you can create, update, or delete a collection of resources by creating, updating, or deleting stacks. All the resources in a stack are defined by the stack's AWS CloudFormation template. A stack, for instance, can include all the resources required to run a web application, such as a web server, a database, and networking rules. If you no longer require that web application, you can

simply delete the stack, and all of its related resources are deleted. You are charged for the stack resources for the time they were operating (even if you deleted the stack right away).
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacks.html

QUESTION 314
In an AWS CloudFormation template, each resource declaration includes:

A. a logical ID, a resource type, and resource properties
B. a variable resource name and resource attributes
C. an IP address and resource entities
D. a physical ID, a resource file, and resource data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, each resource declaration includes three parts: a logical ID that is unique within the template, a resource type, and resource properties.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-resources.html

QUESTION 315 For AWS CloudFormation, which stack state refuses
UpdateStack calls?

A. UPDATE_ROLLBACK_FAILED
B. UPDATE_ROLLBACK_COMPLETE
C. UPDATE_COMPLETE
D. CREATE_COMPLETE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a stack is in the UPDATE_ROLLBACK_FAILED state, you can continue rolling it back to return it to a working state (to UPDATE_ROLLBACK_COMPLETE). You cannot update a stack that is in the UPDATE_ROLLBACK_FAILED state. However, if you can continue to roll it back, you can return the stack to its original settings and try to update it again. http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-continueupdaterollback.html

QUESTION 316 In the context of AWS CloudFormation, which of the following
statements is correct?

A. Actual resource names are a combination of the resource ID, stack, and logical resource name.
B. Actual resource name is the stack resource name.
C. Actual resource name is the logical resource name.
D. Actual resource names are a combination of the stack and logical resource name.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, actual resource names are a combination of the stack and logical resource name. This allows multiple stacks to be created from a template without fear of name collisions between AWS resources.
https://aws.amazon.com/cloudformation/faqs/

QUESTION 317
When using the AWS CLI for AWS CloudFormation, which of the following commands returns a description of the specified resource in the specified stack?

A. describe-stack-events
B. describe-stack-resource
C. create-stack-resource
D. describe-stack-returns

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: awsclicloudformation describe-stack-
resource Description
Returns a description of the specified resource in the specified stack. For deleted stacks, describe-stack-resource returns resource information for up to 90 days after the stack has been deleted.
http://docs.aws.amazon.com/cli/latest/reference/cloudformation/describe-stack-resource.html

QUESTION 318
A user is using CloudFormation to launch an EC2 instance and then configure an application after the instance is launched. The user wants the stack creation of ELB and AutoScaling to wait until the EC2 instance is launched and configured properly.

How can the user configure this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudFormation is an application management tool that provides application modeling, deployment, configuration, management, and related activities. AWS CloudFormation provides a WaitCondition resource that acts as a barrier and blocks the creation of other resources until a completion signal is received from an external source, such as a user application or management system. http://aws.amazon.com/cloudformation/faqs

QUESTION 319
AWS ________supports__________ environments as one of the AWS resource types.

A. Elastic Beanstalk; Elastic Beanstalk application
B. CloudFormation; Elastic Beanstalk application
C. Elastic Beanstalk ; CloudFormation application
D. CloudFormation; CloudFormation application

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudFormation and AWS Elastic Beanstalk services are designed to complement each other. AWS CloudFormation supports Elastic Beanstalk application environments as one of the AWS resource types.
http://aws.amazon.com/cloudformation/faqs/

QUESTION 320
AWS CloudFormation ______ are special actions you use in your template to assign values to properties that are not available until runtime.

A. intrinsic functions
B. properties declarations
C. output functions

D. conditions declarations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS CloudFormation intrinsic functions are special actions you use in your template to assign values to properties not available until runtime. Each function is declared with a name enclosed in quotation marks (""), a single colon, and its parameters. http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-fuctions-structure.html

QUESTION 321 For Amazon EC2 issues, while troubleshooting AWS CloudFormation, you need to view the cloud-init and cfn logs for more information. Identify a directory to which these logs are published.

A. /var/opt/log/ec2
B. /var/log/lastlog
C. /var/log/
D. /var/log/ec2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you use AWS CloudFormation, you might encounter issues when you create, update, or delete AWS CloudFormation stacks.
For Amazon EC2 issues, view the cloud-init and cfn logs. These logs are published on the Amazon EC2 instance in the /var/log/ directory. These logs capture processes and command outputs while AWS CloudFormation is setting up your instance. For Windows, view the EC2Configure service and cfn logs in %ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.
You can also configure your AWS CloudFormation template so that the logs are published to Amazon CloudWatch, which displays logs in the AWS Management Console so you don't have to connect to your Amazon EC2 instance.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html

QUESTION 322
True or false: In a CloudFormation template, you can reuse the same logical ID several times to reference the resources in other parts of the template.

A. True, a logical ID can be used several times to reference the resources in other parts of the template.
B. False, a logical ID must be unique within the template.
C. False, you can mention a resource only once and you cannot reference it in other parts of a template.
D. False, you cannot reference other parts of the template.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, the logical ID must be alphanumeric (A-Za-z0-9) and unique within the template. You use the logical name to reference the resource in other parts of the template.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-resources.html

QUESTION 323 True or false: In CloudFormation, you cannot create an Amazon RDS DB instance from a snapshot.

A. False, you can specify it in attributes
B. False, you can specify it in condition
C. False, you can specify it in resource properties
D. True

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, resource properties are additional options that you can specify on a resource. For example, you can specify the DB snapshot property for an Amazon RDS DB instance in order to create a DB instance from a snapshot. http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-resources.html

QUESTION 324 How can you check the operational validity of your AWS CloudFormation template?

A. To check the operational validity, you need to attempt to create the stack.
B. There is no way to check the operational validity of your AWS CloudFormation template.
C. To check the operational validity, you need a sandbox or test area for AWS CloudFormation stacks.
D. To check the operational validity, you need to use the aws cloudformation validate-template command.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In AWS CloudFormation, to check the operational validity, you need to attempt to create the stack. There is no sandbox or test area for AWS CloudFormation stacks, so you are charged for the resources you create during testing.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-validate-template.html

QUESTION 325 What is a circular dependency in AWS CloudFormation?

A. When Nested Stacks depend on each other.
B. When Resources form a Depend On loop.
C. When a Template references an earlier version of itself.
D. When a Template references a region, which references the original Template.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To resolve a dependency error, add a Depends On attribute to resources that depend on other resources in your template. In some cases, you must explicitly declare dependencies so that AWS CloudFormation can create or delete resources in the correct order. For example, if you create an Elastic IP and a VPC with an Internet gateway in the same stack, the Elastic IP must depend on the Internet gateway attachment. For additional information, see Depends On Attribute.
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html#troubleshooting-errors-dependency-error

QUESTION 326
You need to develop and run some new applications on AWS and you know that Elastic Beanstalk and CloudFormation can both help as a deployment mechanism for a broad range of AWS resources.

Which of the following is TRUE statements when describing the differences between Elastic Beanstalk and CloudFormation?

A. AWS Elastic Beanstalk introduces two concepts: The template, a JSON or YAML-format, text- based file
B. Elastic Beanstalk supports AWS CloudFormation application environments as one of the AWS resource types.
C. Elastic Beanstalk automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. CloudFormation does not.
D. You can design and script custom resources in CloudFormation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
These services are designed to complement each other. AWS Elastic Beanstalk provides an environment to easily deploy and run applications in the cloud. It is integrated with developer tools and provides a one-stop experience for you to manage the lifecycle of your applications. AWS CloudFormation is a convenient provisioning mechanism for a broad range of AWS resources. It supports the infrastructure needs of many different types of applications such as existing enterprise applications, legacy applications, applications built using a variety of AWS resources and container-based solutions (including those built using AWS Elastic Beanstalk). AWS CloudFormation supports Elastic Beanstalk application environments as one of the AWS resource types. This allows you, for example, to create and manage an AWS Elastic Beanstalk- hosted application along with an RDS database to store the application data. In addition to RDS instances, any other supported AWS resource can be added to the group as well. https://aws.amazon.com/cloudformation/faqs

QUESTION 327
An elastic network interface (ENI) is a virtual network interface that you can attach to an instance in a VPC. An ENI can include one public IP address, which can be auto-assigned to the elastic network interface for eth0 when you launch an instance, but only when you_____.

A. create an elastic network interface for eth1
B. include a MAC address
C. use an existing network interface
D. create an elastic network interface for eth0

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An elastic network interface (ENI) is defined as a virtual network interface that you can attach to an instance in a VPC and can include one public IP address, which can be auto-assigned to the elastic network interface for eth0 when you launch an instance, but only when you create an elastic network interface for eth0 instead of using an existing network interface. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 328
After setting an AWS Direct Connect, which of the following cannot be done with an AWS Direct Connect Virtual Interface?

A. You can exchange traffic between the two ports in the same region connecting to different Virtual Private Gateways (VGWs) if you have more than one virtual interface.
B. You can change the region of your virtual interface.
C. You can delete a virtual interface; if its connection has no other virtual interfaces, you can delete the connection.
D. You can create a hosted virtual interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You must create a virtual interface to begin using your AWS Direct Connect connection. You can create a public virtual interface to connect to public resources or a private virtual interface to connect to your VPC. Also, it is possible to configure multiple virtual interfaces on a single AWS Direct Connect connection, and you'll need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key. To use your AWS Direct Connect connection with another AWS account, you can create a hosted virtual interface for that account. These hosted virtual interfaces work the same as standard virtual interfaces and can connect to public resources or a VPC. http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html

QUESTION 329
Identify a correct statement about the expiration date of the "Letter of Authorization and Connecting Facility Assignment (LOA-CFA)," which lets you complete the Cross Connect step of setting up your AWS Direct Connect.

A. If the cross connect is not completed within 90 days, the authority granted by the LOA-CFA expires.
B. If the virtual interface is not created within 72 days, the LOA-CFA becomes outdated.
C. If the cross connect is not completed within a user-defined time, the authority granted by the LOA- CFA expires.
D. If the cross connect is not completed within the specified duration from the appropriate provider, the LOA-CFA expires.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
An AWS Direct Connect location provides access to AWS in the region it is associated with. You can establish connections with AWS Direct Connect locations in multiple regions, but a connection in one region does not provide connectivity to other regions. Note: If the cross connect is not completed within 90 days, the authority granted by the LOA-CFA expires. http://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html

QUESTION 330
Which of the following is the final step that should be completed to start using AWS Direct Connect?

A. Creating your Virtual Interface
B. Configuring your router
C. Completing the Cross Connect
D. Verifying your Virtual Interface

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can get started using AWS Direct Connect by completing the following steps. Step 1: Sign Up for Amazon Web Services Step 2: Submit AWS Direct Connect Connection Request Step 3: Complete the Cross Connect (optional) Step 4: Configure Redundant Connections with AWS Direct Connect Step 5: Create a Virtual Interface Step 6: Download Router Configuration Step 7: Verify Your Virtual Interface
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#connected

QUESTION 331
A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 20.0.1.0/24.

How can the user create the second subnet?

A. The user can modify the first subnet CIDR with AWS CLI
B. The user can modify the first subnet CIDR from the console
C. There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet's CIDR
D. It is not possible to create a second subnet with overlapping IP CIDR without deleting the first subnet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside the subnet. The user can create a subnet with the same size of VPC. However, he cannot create any other subnet since the CIDR of the second subnet will conflict with the first subnet. The user cannot modify the CIDR of a subnet once it is created. Thus, in this case if required, the user has to delete the subnet and create new subnets. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION 332
Which of the following should be followed before connecting to Amazon Virtual Private Cloud (Amazon VPC) using AWS Direct Connect?

A. Provide a public Autonomous System Number (ASN) to identify your network on the Internet.
B. Create a virtual private gateway and attach it to your Virtual Private Cloud (VPC).
C. Allocate a private IP address to your network in the 122.x.x.x range.
D. Provide a public IP address for each Border Gateway Protocol (BGP) session.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To connect to Amazon Virtual Private Cloud (Amazon VPC) by using AWS Direct Connect, you must first do the following:

Provide a private Autonomous System Number (ASN) to identify your network on the Internet. Amazon then allocates a private IP address in the 169.x.x.x range to you. Create a virtual private gateway and attach it to your VPC. http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION 333

Your supervisor has given you the task of creating an elastic network interface on each of your web servers that connect to a mid-tier network where an application server resides. He also wants this set up as a Dual-homed Instance on Distinct Subnets. Instead of routing network packets through the dual-homed instances, where should each dual-homed instance receive and process requests to fulfil his criteria?

A. On one of the web servers
B. On the front end
C. On the back end
D. Through a security group

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can place an elastic network interface on each of your web servers that connects to a mid- tier network where an application server resides. The application server can also be dual-homed to a back-end network (subnet) where the database server resides. If it is set up like this, instead of routing network packets through the dual-homed instances, each dual-homed instance receives and processes requests on the front end and initiates a connection to the back end before finally sending requests to the servers on the back-end network. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 334

A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-123456) to connect to the user's data centre. The user's data centre has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet.

Which of the below mentioned options is not a valid entry for the main route table in this scenario?

A. Destination: 20.0.0.0/16 and Target: local
B. Destination: 0.0.0.0/0 and Target: i-123456
C. Destination: 172.28.0.0/12 and Target: vgw-123456
D. Destination: 20.0.1.0/24 and Target: i-123456

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, he can setup a public and VPN only subnet which uses hardware VPN access to connect with his data centre. When the user has configured this setup with Wizard, it will create a virtual private gateway to route all traffic of the VPN subnet. If the user has setup a NAT instance to route all the internet requests, then all requests to the internet should be routed to it. All requests to the organization's DC will be routed to the VPN gateway. Here are the valid entries for the main route table in this scenario:
Destination: 0.0.0.0/0 & Target: i-123456 (To route all internet traffic to the NAT Instance) Destination: 172.28.0.0/12 & Target: vgw-123456 (To route all the organization's data centre traffic to the VPN gateway)
Destination: 20.0.0.0/16 & Target: local (To allow local routing in VPC) http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html

QUESTION 335 In which step of "start using AWS Direct Connect" steps is the virtual interface you created tagged with a customer-provided tag that complies with the Ethernet 802.1Q standard?

A. Download Router Configuration.
B. Complete the Cross Connect.
C. Configure Redundant Connections with AWS Direct Connect.
D. Create a Virtual Interface.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In the list of using Direct Connect steps, the create a Virtual Interface step is to provision your virtual interfaces. Each virtual interface must be tagged with a customer-provided tag that complies with the Ethernet 802.1Q standard. This tag is required for any traffic traversing the AWS Direct Connect connection. http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#createvirtualinterface

QUESTION 336

A user has created a VPC with CIDR 20.0.0.0/16 using the VPC wizard. The user has created public and VPN only subnets along with hardware VPN access to connect to the user's data centre. The user has not yet launched any instance as well as modified or deleted any setup. He wants to delete this VPC from the console.

Will the console allow the user to delete the VPC?

A. Yes, the user can detach the virtual private gateway and then use the VPC console to delete the VPC.
B. No, since the NAT instance is running, the user cannot delete the VPC.
C. Yes, the user can use the CLI to delete the VPC that will detach the virtual private gateway automatically.
D. No, the VPC console needs to be accessed using an administrator account to delete the VPC.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can delete your VPC at any time (for example, if you decide it's too small). However, you must terminate all instances in the VPC first. When you delete a VPC using the VPC console, Amazon deletes all its components, such as subnets, security groups, network ACLs, route tables, Internet gateways, VPC peering connections, and DHCP options. If you have a VPN connection, you don't have to delete it or the other components related to the VPN (such as the customer gateway and virtual private gateway). http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Deleting

QUESTION 337

You have been asked to set up a public website on AWS with the following criteria:
You want the database and the application server running on an Amazon VPC. You want the database to be able to connect to the Internet so that it can be automatically updated to the correct patch level. You do not want to receive any incoming traffic from the Internet to the database.

Which solutions would be the best to satisfy all the above requirements for your planned public website on AWS? (Choose 2 answers)

A. Set up both the public website and the database on a public subnet and block all incoming requests from the Internet with a Network Access Control List (NACL)
B. Set up both the public website and the database on a public subnet, and block all incoming requests from the Internet with a security group which only allows access from the IP of the public website.
C. Set up the public website on a public subnet and set up the database in a private subnet which connects to the Internet via a NAT instance.
D. Set up both the public website and the database on a private subnet and block all incoming requests from the Internet with a Network Access Control List (NACL). Set up a Security group between the public website and the databasewhich only allows access via port 80.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You want the database to be able to connect to the Internet you need to either set it up on a public subnet or set it up on a private subnet which connects to the Internet via a NAT instance
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 338

Which statement is NOT true about accessing remote AWS region in the US by your AWS Direct Connect which is located in the US?

A. AWS Direct Connect locations in the United States can access public resources in any US region.
B. You can use a single AWS Direct Connect connection to build multi-region services.
C. Any data transfer out of a remote region is billed at the location of your AWS Direct Connect data transfer rate.
D. To connect to a VPC in a remote region, you can use a virtual private network (VPN) connection over your public virtual interface.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

Explanation:
AWS Direct Connect locations in the United States can access public resources in any US region. You can use a single AWS Direct Connect connection to build multi-region services. To connect to a VPC in a remote region, you can use a virtual private network (VPN) connection over your public virtual interface.
To access public resources in a remote region, you must set up a public virtual interface and establish a border gateway protocol (BGP) session. Then your router learns the routes of the other AWS regions in the US. You can then also establish a VPN connection to your VPC in the remote region.
Any data transfer out of a remote region is billed at the remote region data transfer rate.
http://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

QUESTION 339
Which of the following statements is NOT correct when working with your AWS Direct Connect connection after it is set up completely?

A. You can manage your AWS Direct Connect connections and view the connection details.
B. You can delete a connection as long as there are no virtual interfaces attached to it.
C. You cannot view the current connection ID and verify if it matches the connection ID on the Letter of Authorization (LOA).
D. You can accept a host connection by purchasing a hosted connection from the partner (APN).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can manage your AWS Direct Connect connections and view connection details, accept hosted connections, and delete connections. You can view the current status of your connection. You can also view your connection ID, which looks similar to this example dxcon-xxxx, and verify that it matches the connection ID on the Letter of Authorization (LOA) that you received from Amazon. http://docs.aws.amazon.com/directconnect/latest/UserGuide/viewdetails.html

QUESTION 340
Over which of the following Ethernet standards does AWS Direct Connect link your internal network to an AWS Direct Connect location?

A. Single mode fiber-optic cable
B. Multi-mode fiber-optic cable
C. Shielded balanced copper cable
D. Twisted pair cable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet single mode fiber-optic cable.
http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION 341 One of the components that is part of ec2-net-utils used with ENI's is ec2ifscan.

Which of the following is not correct about ec2-net-utils?

A. ec2-net-utils generates an interface configuration file suitable for use with DHCP.
B. ec2-net-utils extends the functionality of the standard if up.
C. ec2-net-utils detaches a primary network interface from an instance.
D. ec2-net-utils identifies network interfaces when they are attached, detached, or reattached to a running instance.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Each instance in a VPC has a default elastic network interface (the primary network interface) that is assigned a private IP address from the IP address range of your VPC. You cannot detach a primary network interface from an instance.

You can create and attach additional elastic network interfaces. Amazon Linux AMIs may contain additional scripts installed by AWS, known as ec2-net-utils. One of the components that is part of ec2-net-utils used with ENI's is ec2ifscan. Its function is to check for network interfaces that have not been configured and configure them.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 342
A user wants to create a public subnet in VPC and launch an EC2 instance within it. The user has not selected the option to assign a public IP address while launching the instance.

Which of the below mentioned statements is true with respect to this scenario?

A. The instance will always have a public DNS attached to the instance by default
B. The user would need to create a default route to IGW in subnet's route table and then attach an elastic IP to the instance to connect from the internet
C. The user can directly attach an elastic IP to the instance
D. The instance will never launch if the public IP is not assigned

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When the user is launching an instance he needs to select an option which attaches a public IP to the instance. If the user has not selected the option to attach the public IP, then it will only have a private IP when launched. The user cannot connect to the instance from the internet. If the user wants an elastic IP to connect to the instance from the internet, he should create an internet gateway and assign an elastic IP to instance.
http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/LaunchInstance.html

QUESTION 343
A user has created a VPC with a public subnet. The user has terminated all the instances which are part of the subnet.

Which of the below mentioned statements is true with respect to this scenario?

A. The subnet to which the instances were launched with will be deleted
B. When the user launches a new instance it cannot use the same subnet
C. The user cannot delete the VPC since the subnet is not deleted
D. Secondary network interfaces attached to the terminated instances may persist.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. When an instance is launched it will have a network interface attached with it. The user cannot delete the subnet until he terminates the instance and deletes the network interface. By default, network interfaces that are automatically created and attached to instances using the console are set to terminate when the instance terminates. However, network interfaces created using the command line interface aren't set to terminate when the instance terminates. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 344 When configuring your customer gateway to connect to your VPC, the________Association is established first between the virtual private gateway and customer gateway using the Pre-Shared Key as the authenticator.

A. IPsec
B. BGP
C. IKE Security
D. Tunnel

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
When configuring your customer gateway to connect to your VPC, several steps need to be completed. The IKE Security Association is established first between the virtual private gateway and customer gateway using the Pre-Shared Key as the authenticator. http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html

QUESTION 345
An organization is trying to setup a VPC with Auto Scaling. Which configuration steps below is not required to setup AWS VPC with Auto Scaling?

A. Configure the Auto Scaling group with the VPC ID in which instances will be launched.
B. Configure the Auto Scaling Launch configuration with multiple subnets of the VPC to enable the Multi AZ feature.
C. Configure the Auto Scaling Launch configuration which does not allow assigning a public IP to instances.
D. Configure the Auto Scaling Launch configuration with the VPC security group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Within this virtual private cloud, the user can launch AWS resources, such as an Auto Scaling group. Before creating the Auto Scaling group it is recommended that the user creates the Launch configuration. Since it is a VPC, it is recommended to select the parameter which does not allow assigning a public IP to the instances.
The user should also set the VPC security group with the Launch configuration and select the subnets where the instances will be launched in the AutoScaling group. The HA will be provided as the subnets may be a part of separate AZs.
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/autoscalingsubnets.html

QUESTION 346
An organization is planning to host a Wordpress blog as well as joomla CMS on a single instance launched with VPC. The organization wants to create separate domains for each application using Route 53. The organization may have about ten instances each with these two applications. While launching each instance, the organization configured two separate network interfaces (primary + secondary ENI) with their own Elastic IPs to the instance. The suggestion was to use a public IP from AWS instead of an Elastic IP as the number of elastic IPs allocation per region is restricted in the account.

What action will you recommend to the organization?

A. Only Elastic IP can be used by requesting limit increase, since AWS does not assign a public IP to an instance with multiple ENIs.
B. AWS VPC does not attach a public IP to an ENI; so the only way is to use an Elastic IP.
C. I agree with the suggestion but will prefer that the organization should use separate subnets with each ENI for different public IPs.
D. I agree with the suggestion and it is recommended to use a public IP from AWS since the organization is going to use DNS with Route 53.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. An Elastic Network Interface (ENI) is a virtual network interface that the user can attach to an instance in a VPC.
The user can attach up to two ENIs with a single instance. However, AWS cannot assign a public IP when there are two ENIs attached to a single instance. It is recommended to assign an elastic IP in this scenario. If the organization wants more than 5 EIPs they can request AWS to increase the number. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 347
A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance.

Which of the below mentioned entries is not required in NAT's security group for the database servers to connect to the Internet for software updates?

A. For Outbound allow Destination: 0.0.0.0/0 on port 443
B. For Inbound allow Source: 20.0.1.0/24 on port 80
C. For Inbound allow Source: 20.0.0.0/24 on port 80
D. For Outbound allow Destination: 0.0.0.0/0 on port 80

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet to host the web server and DB server respectively, the user should configure that the instances in the private subnet can connect to the internet using the NAT instances. The user should first configure that NAT can receive traffic on ports 80 and 443 from the private subnet. Thus, allow ports 80 and 443 in Inbound for the private subnet 20.0.1.0/24. Now to route this traffic to the internet configure ports 80 and 443 in Outbound with destination 0.0.0.0/0. The NAT should not have an entry for the public subnet CIDR.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 348
A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is true in this scenario?

A. The user has to manually create a NAT instance
B. The Amazon VPC will automatically create a NAT instance with the micro size only
C. VPC updates the main route table used with the private subnet, and creates a custom route table with a public subnetD. VPC updates the main route table used with a public subnet, and creates a custom route table with a private subnet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public subnet, the instances in the public subnet can receive inbound traffic directly from the internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create a NAT instance of a smaller or higher size, respectively. The VPC has an implied router and the VPC wizard updates the main route table used with the private subnet, creates a custom route table and associates it with the public subnet.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 349
A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet.

How can the instances in the private subnet connect to the internet?

A. The private subnet can never connect to the internet
B. Use NAT with an elastic IP
C. Use the internet gateway with a private IP
D. Allow outbound traffic in the security group for port 80 to allow internet updates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created two subnets (one private and one public), they would need a Network Address Translation (NAT) instance with the elastic IP address. This enables the instances in the private subnet to send requests to the internet (for example, to perform software updates).
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 350
A user has created a VPC with public and private subnets using the VPC Wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24.

Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?

A. Destination : 20.0.0.0/0 and Target : ALL
B. Destination : 20.0.0.0/16 and Target : Local C. Destination : 20.0.0.0/24 and Target : Local
D. Destination : 20.0.0.0/16 and Target : ALL

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user can create a subnet with VPC and launch instances inside that subnet. If the user has created a public private subnet, the instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet cannot. If these subnets are created with Wizard, AWS will create two route tables and attach to the subnets. The main route table will have the entry "Destination: 20.0.0.0/16 and Target: Local", which allows all instances in the VPC to communicate with each other. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

QUESTION 351
You want to establish redundant VPN connections and customer gateways on your network by setting up a second VPN connection.

Which of the following will ensure that this functions correctly?

A. The customer gateway IP address for the second VPN connection must be publicly accessible.
B. The virtual gateway IP address for the second VPN connection must be publicly accessible.
C. The customer gateway IP address for the second VPN connection must use dynamic routes.
D. The customer gateway IP address for the second VPN connection must be privately accessible and be the same public IP address that you are using for the first VPN connection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To establish redundant VPN connections and customer gateways on your network, you would need to set up a second VPN connection. However, you must ensure that the customer gateway IP address for the second VPN connection is publicly accessible.
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

QUESTION 352
Someone is creating a VPC for their application hosting. He has created two private subnets in the same availability zone and created one subnet in a separate availability zone. He wants to make a High Availability system with an internal Elastic Load Balancer.

Which choice is true regarding internal ELBs in this scenario? (Choose 2 answers)

A. Internal ELBs should only be launched within private subnets.
B. Amazon ELB service does not allow subnet selection; instead it will automatically select all the available subnets of the VPC.
C. Internal ELBs can support only one subnet in each availability zone.
D. An internal ELB can support all the subnets irrespective of their zones.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Within this virtual private cloud, the user can launch AWS resources, such as elastic load balancers, and EC2 instances. There are two ELBs available with VPC: internet facing and internal (private) ELB. For internal servers, such as App servers the organization can create an internal load balancer in their VPC and then place back-end application instances behind the internal load balancer. The internal load balancer will route requests to the back-end application instances, which are also using private IP addresses and only accept requests from the internal load balancer. The Internal ELB supports only one subnet in each AZ and asks the user to select a subnet while configuring internal ELB. http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/USVPC_creating_basic_lb.html

QUESTION 353
To ensure failover capabilities on an elastic network interface (ENI), what should you use for incoming traffic?

A. A Route53 A record
B. A secondary private IP
C. A secondary public IP

D. A secondary ENI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To ensure failover capabilities on an elastic network interface (ENI), consider using a secondary private IP for incoming traffic and if a failure occurs, you can move the interface and/or secondary private IP address to a standby instance.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 354
An organization is setting up a highly scalable application using Elastic Beanstalk. The organization is using ELB and RDS with VPC. The organization has public and private subnets within the cloud.

Which of the below mentioned configurations will not work in this scenario?

A. To setup RDS in a private subnet and ELB in a public subnet.
B. The configuration must have public and private subnets in the same AZ.
C. The configuration must have two private subnets in separate AZs.
D. The EC2 instance should have a public IP assigned to it.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. If the organization is planning to implement a scalable secure application using RDS, VPC and ELB the organization should follow below mentioned configurations: Setup RDS in a private subnet Setup ELB in a public subnet
Since RDS needs a subnet group, the organization should have two private subnets in the same zone
The ELB needs private and public subnet to be part of same AZs It is not required that instances should have a public IP assigned to them. The instances can be a part of a private subnet and the organization can setup a corresponding routing mechanism. http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/vpc-rds.html

QUESTION 355 In DynamoDB, a projection is__________.

A. systematic transformation of the latitudes and longitudes of the locations inside your table
B. importing data from your file to a table
C. exporting data from a table to your file
D. the set of attributes that is copied from a table into a secondary index

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In DynamoDB, a projection is the set of attributes that is copied from a table into a secondary index.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GSI.html

QUESTION 356
Which of the following is NOT true of the DynamoDB Console?
A. It allows you to add local secondary indexes to existing tables.
B. It allows you to query a table.
C. It allows you to set up alarms to monitor your table's capacity usage.
D. It allows you to view items stored in a tables, add, update, and delete items.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The DynamoDB Console lets you do the following: Create, update, and delete tables. The throughput calculator provides you with estimates of how many capacity units you will need to request based on the usage information you provide. View items stored in a tables, add, update, and delete items. Query a table. Set up alarms to monitor your table's capacity usage. View your table's top monitoring metrics on real-time graphs from CloudWatch. View alarms configured for each table and create custom alarms.html.

QUESTION 357 DynamoDB usesonly as a transport protocol, not as
a storage format.

A. WDDX
B. XML
C. SGML
D. JSON

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DynamoDB uses JSON only as a transport protocol, not as a storage format. The AWS SDKs use JSON to send data to DynamoDB, and DynamoDB responds with JSON, but DynamoDB does not store data persistently in JSON format.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Programming.LowLev elAPI.html

QUESTION 358
In DynamoDB, which of the following allows you to set alarms when you reach a specified threshold for a metric?

A. Alarm Signal
B. DynamoDB Analyzer
C. CloudWatch
D. DynamoDBALARM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudWatch allows you to set alarms when you reach a specified threshold for a metric.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/MonitoringDynamoDB.html

QUESTION 359 Is it possible to load data from Amazon DynamoDB into
Amazon Redshift?

A. No, you cannot load all the data from DynamoDB table to a Redshift table as it limited by size constraints.
B. No
C. No, DynamoDB data types do not correspond directly with those of Amazon Redshift.
D. Yes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Yes. When you copy data from an Amazon DynamoDB table into Amazon Redshift, you can perform complex data analysis queries on that data. This includes joins with other tables in your Amazon Redshift cluster.

http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/RedshiftforDynamoDB.html

QUESTION 360 In regard to DynamoDB, when you create a table with a
hash-and-range key.

A. You must define one or more Local secondary indexes on that table
B. You must define one or more Global secondary indexes on that table
C. You can optionally define one or more secondary indexes on that table
D. You must define one or more secondary indexes on that table

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you create a table with a hash-and-range key, you can optionally define one or more secondary indexes on that table. A secondary index lets you query the data in the table using an alternate key, in addition to queries against the primary key. http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DataModel.html

QUESTION 361
Someone has recommended a new client to you and you know he is into online gaming and you are almost certain he will want to set up an online gaming site which will require a database service that provides fast and predictable performance with seamless scalability.

Which of the following AWS databases would be best suited to an online gaming site?

A. Amazon SimpleDB
B. Amazon DynamoDB
C. Amazon Redshift
D. Amazon ElastiCache

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. You can use Amazon DynamoDB to create a database table that can store and retrieve any amount of data, and serve any level of request traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified by the customer and the amount of data stored, while maintaining consistent and fast performance. http://aws.amazon.com/documentation/dynamodb/

QUESTION 362 In DynamoDB, "The data is eventually consistent" means
that__________.

A. a read request immediately after a write operation might not show the latest change.
B. a read request immediately after a write operation shows the latest change.
C. a write request immediately after a read operation might cause data loss.D. a read request immediately after a write operation might cause data loss.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In DynamoDB, it takes time for the update to propagate to all copies. The data is eventually consistent, meaning that a read request immediately after a write operation might not show the latest change.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html

QUESTION 363
____________pricing offers significant savings over the normal price of DynamoDB provisioned throughput capacity.

A. Discount Voucher
B. Reserved Capacity
C. Discount Service
D. Reserved Point

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reserved Capacity pricing offers significant savings over the normal price of DynamoDB provisioned throughput capacity. When you buy Reserved Capacity, you pay a one-time upfront fee and commit to paying for a minimum usage level, at the hourly rates indicated above, for the duration of the Reserved Capacity term. http://aws.amazon.com/dynamodb/pricing/

QUESTION 364 In DynamoDB, which of the following operations is not possible by the console?

A. Updating an item
B. Copying an item
C. Blocking an item
D. Deleting an item

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By using the console to manage DynamoDB, you can perform the following: adding an item, deleting an item, updating an item, and copying an item.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AddUpdateDeleteItems.html

QUESTION 365 In order for a table write to succeed, the provisioned throughput settings for the table and global secondary indexes, in DynamoDB, must have__________; otherwise, the write to the table will be throttled.

A. enough write capacity to accommodate the write
B. no additional write cost for the index
C. 100 bytes of overhead per index item
D. the size less than or equal to 1 KB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order for a table write to succeed in DynamoDB, the provisioned throughput settings for the table and global secondary indexes must have enough write capacity to accommodate the write; otherwise, the write will be throttled.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GSI.html

QUESTION 366 In DynamoDB, to get a detailed listing of secondary indexes on a table, you can use the ______ action.

A. BatchGetItem
B. TableName
C. DescribeTable
D. GetItem

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In DynamoDB, DescribeTable returns information about the table, including the current status of the table, when it was created, the primary key schema, and any indexes on the table.
http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html

QUESTION 367 In regard to DynamoDB, for which one of the following parameters does Amazon
not charge you?

A. Storage cost
B. I/O usage within the same Region
C. Cost per provisioned read units
D. Cost per provisioned write units

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In DynamoDB, you will be charged for the storage and the throughput you use rather than for the I/O which has been used.
http://aws.amazon.com/dynamodb/pricing/

QUESTION 368
Complete this statement: "When you load your table directly from an Amazon_____ table, you have the option to control the amount of provisioned throughput you consume."

A. RDS
B. DataPipeline
C. DynamoDB
D. S3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When you load your table directly from an Amazon DynamoDB table, you have the option to control the amount of Amazon DynamoDB provisioned throughput you consume.
http://docs.aws.amazon.com/redshift/latest/dg/t_Loading_tables_with_the_COPY_command.html

QUESTION 369
Which of the following does Amazon DynamoDB perform?

A. Atomic increment or decrement on scalar values
B. Neither increment nor decrement operations
C. Only increment on vector values
D. Only atomic decrement operations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: Amazon DynamoDB allows atomic increment and decrement operations on scalar values. http://aws.amazon.com/dynamodb/faqs/

QUESTION 370 A Provisioned IOPS volume must be at least
__________ GB in size:

A. 20 B.
10
C. 50
D. 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Provisioned IOPS volume must be at least 10 GB in size
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

QUESTION 371
A user has launched two EBS backed EC2 instances in the US-East-1a region. The user wants to change the zone of one of the instances. How can the user change it?

A. It is not possible to change the zone of an instance after it is launched
B. From the AWS EC2 console, select the Actions - > Change zones and specify the new zone
C. The zone can only be modified using the AWS CLI
D. Stop one of the instances and change the availability zone

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With AWS EC2, when a user is launching an instance he can select the availability zone (AZ) at the time of launch. If the zone is not selected, AWS selects it on behalf of the user. Once the instance is launched, the user cannot change the zone of that instance unless he creates an AMI of that instance and launches a new instance from it. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

QUESTION 372 In Amazon Elastic Compute Cloud, you can specify storage volumes in addition to the root device volume when you create an AMI or when launching a new instance using______.

A. block device mapping
B. object mapping
C. batch storage mapping
D. datacenter mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When creating an AMI or launching a new instance, you can assign more than one block storage device to it.
This device will be automatically set ready for you through an automated process known as block device mapping.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html

QUESTION 373 You create an Amazon Elastic File System (EFS) file system and mount targets for the file system in your Virtual Private Cloud (VPC). Identify the initial permissions you can grant to the group root of your file system.

A. write-execute-modify
B. read-execute
C. read-write-modify
D. read-write

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Amazon EFS, when a file system and mount targets are created in your VPC, you can mount the remote file system locally on your Amazon Elastic Compute Cloud (EC2) instance. You can grant permissions to the users of your file system. The initial permissions mode allowed for Amazon EFS are:

▪ read-write-execute permissions to the owner root
▪ read-execute permissions to the group root read-execute permissions to others http://docs.aws.amazon.com/efs/latest/ug/accessing-fs-nfs-permissions.html

QUESTION 374
You want to mount an Amazon EFS file system on an Amazon EC2 instance using DNS names. Which of the following generic form of a mount target's DNS name must you use to mount the file system?

A. availability-zone.file-system-id.efs.aws-region.amazonaws.com
B. efs-system-id.availability-zone.file-aws-region.amazonaws.com
C. $file-system-id.$availability-zone.$efs.aws-region.$amazonaws.com
D. #aws-region.#availability-zone.#file-system-id.#efs.#amazonaws.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An Amazon EFS file system can be mounted on an Amazon EC2 instance using DNS names. This can be done with either a DNS name for the file system or a DNS name for the mount target. To construct the mount target's DNS name, use the following generic form:
availability-zone.file-system-id.efs.aws-region.amazonaws.com http://docs.aws.amazon.com/efs/latest/ug/mounting-fs.html#mounting-fs-install-nfsclient

QUESTION 375
A user is creating a Provisioned IOPS volume. What is the maximum ratio the user should configure between Provisioned IOPS and the volume size?

A. 30 to 1 B.
50 to 1 C.
10 to 1
D. 20 to 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. An io1 volume can range in size from 4 GiB to 16 TiB and you can provision 100 up to 20,000 IOPS per volume. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1. For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS. Any volume 400 GiB in size or greater allows provisioning up to the 20,000 IOPS maximum.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

QUESTION 376
Your Application is not highly available, and your on-premises server cannot access the mount target because the Availability Zone (AZ) in which the mount target exists is unavailable.

Which of the following actions is recommended?

A. The application must implement the checkpoint logic and recreate the mount target.
B. The application must implement the shutdown logic and delete the mount target in the AZ.
C. The application must implement the delete logic and connect to a different mount target in the same AZ.
D. The application must implement the restart logic and connect to a mount target in a different AZ.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To make sure that there is continuous availability between your on-premises data center and your Amazon Virtual Private Cloud (VPC), it is suggested that you configure two AWS Direct Connect connections. Your application should implement restart logic and connect to a mount target in a different AZ if your application is not highly available and your on-premises server cannot access the mount target because the AZ in which the mount target exists becomes unavailable. http://docs.aws.amazon.com/efs/latest/ug/performance.html#performance-onpremises

QUESTION 377
Which of the following Amazon RDS storage types is ideal for applications with light or burst I/O requirements?

A. Both magnetic and Provisioned IOPS storage
B. Magnetic storage
C. Provisioned IOPS storage
D. None of these

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon RDS provides three storage types: magnetic, General Purpose (SSD), and Provisioned IOPS (input/output operations per second). Magnetic (Standard) storage is ideal for applications with light or burst I/O requirements.
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

QUESTION 378
When I/O performance is more important than fault tolerance, which of the following configurations should be used?

A. SPAN 10
B. RAID 1C. RAID 0
D. NFS 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When I/O performance is more important than fault tolerance, the RAID 0 configuration must be used; for example, as in a heavily used database (where data replication is already set up separately).
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

QUESTION 379
Amazon Elastic File System (EFS) provides information about the space used for an object by using the space _ used attribute of the Network File System Version 4.1 (NFSv4.1). The attribute includes the object's current metered data size and not the metadata size. Which of the following utilities will you use to measure the amount of disk that is used of a file?

A. blkid utility
B. du utility
C. sfdisk utility
D. pydf utility

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Amazon EFS reports file system sizes and sizes of objects within a file system. Using the NFSv4.1 space _ used attribute for measuring the space used for an object, it reports only the object's current metered data size and not the metadata size. There are two utilities available for measuring disk usage of a file, the du and stat utilities. https://docs.aws.amazon.com/efs/latest/ug/metered-sizes.html

QUESTION 380

You have custom Network File System (NFS) client settings for your Amazon Elastic File System (EFS). It takes up to three seconds for an Amazon Elastic Compute Cloud (EC2) instance to see a write operation performed on a file system from another Amazon EC2 instance.

Which of the following actions should you take to solve the custom NFS settings from causing delays in the write operation?

A. Unmount and remount the file system with the noac option to disable attribute caching.
B. Reduce the number of active users that have files open simultaneously on the instances.
C. Verify that the IP address of the specified mount target is valid.
D. Run the write operation from a different user ID on the same Amazon EC2 instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

When you set up custom NFS client settings, it takes up to three seconds for an Amazon EC2 instance to see a write operation being performed on a file system from another Amazon EC2 instance. To solve this issue, you must unmount and remount your file system with the noac option to disable attribute caching if the NFS client on the Amazon EC2 instance that is reading the data has attribute caching activated. Attribute cache can also be cleared on demand by using a programming language that is compatible with the NFS procedures. To do this, you must send an ACCESS procedure request immediately before a read request. http://docs.aws.amazon.com/efs/latest/ug/troubleshooting.html#custom-nfs-settings-write-delays

QUESTION 381

Which of the following rules must be added to a mount target security group to access Amazon Elastic File System (EFS) from an on-premises server?

A. Configure an NFS proxy between Amazon EFS and the on-premises server to route traffic.
B. Set up a Point-To-Point Tunneling Protocol Server (PPTP) to allow secure connection.
C. Permit secure traffic to the Kerberos port 88 from the on-premises server.
D. Allow inbound traffic to the Network File System (NFS) port (2049) from the on-premises server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

By mounting an Amazon EFS file system on an on-premises server, on-premises data can be migrated into the AWS Cloud. Any one of the mount targets in your VPC can be used as long as the subnet of the mount target is reachable by using the AWS Direct Connect connection. To access Amazon EFS from an on-premises server, a rule must be added to the mount target security group to allow inbound traffic to the NFS port (2049) from the on-premises server. http://docs.aws.amazon.com/efs/latest/ug/how-it-works.html

QUESTION 382

Which of the following is true of Amazon EBS encryption keys?

A. Amazon EBS encryption uses the Customer Master Key (CMK) to create an AWS Key Management Service (AWS KMS) master key.
B. Amazon EBS encryption uses the EBS Magnetic key to create an AWS Key Management Service (AWS KMS) master key.
C. Amazon EBS encryption uses the EBS Magnetic key to create a Customer Master Key (CMK).
D. Amazon EBS encryption uses the AWS Key Management Service (AWS KMS) master key to create a Customer Master Key (CMK).

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Amazon EBS encryption uses AWS Key Management Service (AWS KMS) master keys when creating encrypted volumes and any snapshots created from your encrypted volumes.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html

QUESTION 383
A user is creating a snapshot of an EBS volume. Which of the below statements is incorrect in relation to the creation of an EBS snapshot?

A. Its incremental
B. It is a point in time backup of the EBS volume
C. It can be used to create an AMI
D. It is stored in the same AZ as the volume

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The EBS snapshots are a point in time backup of the EBS volume. It is an incremental snapshot, but is always specific to the region and never specific to a single AZ. Hence the statement "It is stored in the same AZ as the volume" is incorrect. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

QUESTION 384
A user is running a critical batch process which runs for 1 hour and 50 mins every day at a fixed time. 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. Instance store backed instance with spot instance pricing.
B. EBS backed instance with standard reserved upfront instance pricing.
C. EBS backed scheduled reserved instance with partial instance pricing.
D. EBS backed instance with on-demand instance pricing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For Amazon Web Services, the reserved instance (standard or convertible) 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% of the year annually it is recommended to use RI. Here as the instance runs only for 1 hour 50 minutes daily, or less than 8 percent of the year, it is not recommended to have RI as it will be costlier. At its highest potential savings, you are still paying 25 percent of an annual cost for a reserved instance you are you using less than 2 hours a day, (or less than 8 percent of each year) you are not saving money. Even a scheduled reserved instance has a key limitation, which is that it cannot be stopped or rebooted, only manually terminated with a possibility that it could be restarted. You would have to terminate and restart it within the 1 hour 50-minute window, otherwise you would need to wait until the next day. For a critical daily process, this is likely not an option. Spot Instances are not ideal because the process is critical, and must run for a fixed length of time at a fixed time of day. Spot instances would stop and start based on fluctuations in instance pricing, leaving this process potentially unfinished. The user should use on-demand with EBS in this case. While it has the highest cost, it also has the greatest flexibility to ensure that a critical process like this is always completed.
http://aws.amazon.com/ec2/purchasing-options/reserved-instances/

QUESTION 385
A user has created a launch configuration for Auto Scaling where CloudWatch detailed monitoring is disabled. The user wants to now enable detailed monitoring.
How can the user achieve this?

A. Update the Launch config with CLI to set InstanceMonitoringDisabled = false
B. The user should change the Auto Scaling group from the AWS console to enable detailed monitoring
C. Create a new Launch Config with detail monitoring enabled and update the Auto Scaling groupD. Update the Launch config with CLI to set InstanceMonitoring.Enabled = true

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

CloudWatch is used to monitor AWS as well as the custom services. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates the Auto Scaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. When the user has created a launch configuration with InstanceMonitoring.Enabled = false it will involve multiple steps to enable detail monitoring. The steps are:

- Create a new Launch config with detailed monitoring enabled
- Update the Auto Scaling group with a new launch config
- Enable detail monitoring on each EC2 instance http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/as-metricscollected.html

QUESTION 386

A user is sending a custom metric to CloudWatch. If the call to the CloudWatch APIs has different dimensions, but the same metric name, how will CloudWatch treat all the requests?

A. It will reject the request as there cannot be a separate dimension for a single metric.
B. It will group all the calls into a single call.
C. It will treat each unique combination of dimensions as a separate metric.
D. It will overwrite the previous dimension data with the new dimension data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A dimension is a key-value pair used to uniquely identify a metric. CloudWatch treats each unique combination of dimensions as a separate metric.
Thus, if the user is making 4 calls with the same metric name but a separate dimension, it will create 4 separate metrics.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION 387

What is the maximum number of data points for an HTTP data request that a user can include in PutMetricRequest in the CloudWatch?

A. 30
B. 50
C. 10
D. 20

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The size of a PutMetricData request of CloudWatch is limited to 8KB for the HTTP GET requests and 40KB for the HTTP POST requests. The user can include a maximum of 20 data points in one PutMetricData request.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION 388

You have set up a huge amount of network infrastructure in AWS and you now need to think about monitoring all of this. You decide CloudWatch will best fit your needs but you are unsure of the pricing structure and the limitations of CloudWatch.

Which of the following statements is TRUE in relation to the limitations of CloudWatch?

A. You get 10 CloudWatch metrics, 10 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per customer per month for free.
B. You get 100 CloudWatch metrics, 100 alarms, 10,000,000 API requests, and 10,000 Amazon SNS email notifications per customer per month for free.
C. You get 10 CloudWatch metrics, 10 alarms, 1,000 API requests, and 100 Amazon SNS email notifications per customer per month for free.
D. You get 100 CloudWatch metrics, 100 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per customer per month for free.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications.
CloudWatch has the following limits:
You get 10 CloudWatch metrics, 10 alarms, 1,000,000 API requests, and 1,000 Amazon SNS email notifications per customer per month for free. You can assign up to 10 dimensions per metric.
You can create up to 5000 alarms per AWS account. Metric data is kept for 2 weeks.
The size of a PutMetricData request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests.
You can include a maximum of 20 MetricDatum items in one PutMetricData request. A MetricDatum can contain a single value or a StatisticSet representing many values.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_limits.html

QUESTION 389
A user is trying to send custom metrics to CloudWatch using the PutMetricData APIs. Which of the below mentioned points should the user needs to take care while sending the data to CloudWatch?

A. The size of a request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests
B. The size of a request is limited to 16KB for HTTP GET requests and 80KB for HTTP POST requests
C. The size of a request is limited to 128KB for HTTP GET requests and 64KB for HTTP POST requestsD. The size of a request is limited to 40KB for HTTP GET requests and 8KB for HTTP POST requests

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With AWS CloudWatch, the user can publish data points for a metric that share not only the same time stamp, but also the same namespace and dimensions. CloudWatch can accept multiple data points in the same PutMetricData call with the same time stamp. The only thing that the user needs to take care of is that the size of a PutMetricData request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION 390 You set up your first Lambda function and want to set up some Cloudwatch metrics to monitor your function. Which of the following Lambda metrics can Cloudwatch monitor?

A. Total requests only
B. Status Check Failed, total requests, and error rates
C. Total requests and CPU utilization
D. Total invocations, errors, duration, and throttles

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Lambda automatically monitors functions on your behalf, reporting metrics through Amazon CloudWatch (CloudWatch). These metrics include total invocations, errors, duration, and throttles.
http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-metrics.html

QUESTION 391 How many metrics are supported by CloudWatch for Auto Scaling?

A. 7 metrics and 5 dimension
B. 5 metrics and 1 dimension
C. 1 metric and 5 dimensionsD. 8 metrics and 1 dimension

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

AWS Auto Scaling supports both detailed as well as basic monitoring of the CloudWatch metrics. Basic monitoring happens every 5 minutes, while detailed monitoring happens every minute. It supports 8 metrics and 1 dimension.
The metrics are: GroupMinSize GroupMaxSize GroupDesiredCapacity GroupInServiceInstances GroupPendingInstances GroupStandbyInstances GroupTerminatingInstances GroupTotalInstances
The dimension is AutoScalingGroupName
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION 392 A user has enabled detailed CloudWatch monitoring with the AWS Simple Notification Service. Which of the below mentioned statements helps the user understand detailed monitoring better?

A. SNS cannot provide data every minute
B. SNS will send data every minute after configuration
C. There is no need to enable since SNS provides data every minute
D. AWS CloudWatch does not support monitoring for SNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. The AWS SNS service sends data every 5 minutes. Thus, it supports only the basic monitoring. The user cannot enable detailed monitoring with SNS.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION 393
An AWS account owner has setup multiple IAM users. One of these IAM users, named John, has CloudWatch access, but no access to EC2 services. John has setup an alarm action which stops EC2 instances when their CPU utilization is below the threshold limit.

When an EC2 instance's CPU Utilization rate drops below the threshold John has set, what will happen and why?

A. CloudWatch will stop the instance when the action is executed
B. Nothing will happen. John cannot set an alarm on EC2 since he does not have the permission.
C. Nothing will happen. John can setup the action, but it will not be executed because he does not have EC2 access through IAM policies.D. Nothing will happen because it is not possible to stop the instance using the CloudWatch alarm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which stops the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action. If the IAM user has read/write permissions for Amazon CloudWatch but not for Amazon EC2, he can still create an alarm. However, the stop or terminate actions will not be performed on the Amazon EC2 instance.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

QUESTION 394
A user has configured an EC2 instance in the US-East-1a zone. The user has enabled detailed monitoring of the instance. The user is trying to get the data from CloudWatch using a CLI.

Which of the below mentioned CloudWatch endpoint URLs should the user use?

A. monitoring.us-east-1a.amazonaws.com
B. cloudwatch.us-east-1a.amazonaws.com
C. monitoring.us-east-1.amazonaws.com
D. monitoring.us-east-1-a.amazonaws.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The CloudWatch resources are always region specific and they will have the end point as region specific. If the user is trying to access the metric in the US-East-1 region, the endpoint URL will be: monitoring.us-east-1.amazonaws.com
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/regions_endpoints.html

QUESTION 395 Which of the following is not included in the metrics sent from Billing to Amazon CloudWatch?

A. Recurring fees for AWS products and services
B. Total AWS charges
C. One-time charges and refunds
D. Usage charges for AWS products and services

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Usage charges and recurring fees for AWS products and services are included in the metrics sent from Billing to Amazon CloudWatch. You will have a metric for total AWS charges, as well as one additional metric for each AWS product or service that you use.
However, one-time charges and refunds are not included.
https://aws.amazon.com/blogs/aws/monitor-estimated-costs-using-amazon-cloudwatch-billing-metrics-and-alarms

QUESTION 396
After your Lambda function has been running for some time, you need to look at some metrics to ascertain how your function is performing and decide to use the AWS CLI to do this.

Which of the following commands must be used to access these metrics using the AWS CLI?

A. mon-list-metrics and mon-get-stats
B. list-metrics and get-metric-statistics
C. ListMetrics and GetMetricStatistics
D. list-metrics and mon-get-stats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AWS Lambda automatically monitors functions on your behalf, reporting metrics through Amazon CloudWatch.
To access metrics using the AWS CLI
Use the list-metrics and get-metric-statistics commands.
http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-access-metrics.html

QUESTION 397
In Amazon CloudWatch, you can publish your own metrics with the put-metric-data command. When you create a new metric using the put-metric-data command, it can take up to two minutes before you can retrieve statistics on the new metric using the get-metric-statistics command.

How long does it take before the new metric appears in the list of metrics retrieved using the list- metrics command?

A. After 2 minutes
B. Up to 15 minutes
C. More than an hour
D. Within a minute

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can publish your own metrics to CloudWatch with the put-metric-data command (or its Query API equivalent PutMetricData). When you create a new metric using the put-metric-data command, it can take up to two minutes before you can retrieve statistics on the new metric using the get-metric-statistics command. However, it can take up to fifteen minutes before the new metric appears in the list of metrics retrieved using the list-metrics command.
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION 398
A company runs a legacy system on a single m4.2xlarge Amazon EC2 instance with Amazon EBS2 storage. The EC2 instance runs both the web server and a self-managed Oracle database. A snapshot is made of the EBS volume every 12 hours, and an AMI was created from the fully configured EC2 instance.
A recent event that terminated the EC2 instance led to several hours of downtime. The application was successfully launched from the AMI, but the age of the EBS snapshot and the repair of the database resulted in the loss of 8 hours of data. The system was also down for 4 hours while the Systems Operators manually performed these processes. What architectural changes will minimize downtime and reduce the chance of lost data?

A. Create an Amazon CloudWatch alarm to automatically recover the instance. Create a script that will check and repair the database upon reboot. Subscribe the Operations team to the Amazon SNS message generated by theCloudWatch alarm.
B. Run the application on m4.xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of two.Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.
C. Run the application on m4.2xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group access multiple Availability Zones with a minimum instance count of one.Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.
D. Increase the web server instance count to two m4.xlarge instances and use Amazon Route 53 round-robin load balancing to spread the load. Enable Route 53 health checks on the web servers. Migrate the database to an Amazon RDSOracle Multi-AZ DB instance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 399
A Solutions Architect is working with a company that operates a standard three-tier web application in AWS. The web and application tiers run on Amazon EC2 and the database tier runs on Amazon RDS. The company is redesigning the web and application tiers to use Amazon API Gateway and AWS Lambda, and the company intends to deploy the new application within 6 months. The IT Manager has asked the Solutions Architect to reduce costs in the interim.

Which solution will be MOST cost effective while maintaining reliability?

A. Use Spot Instances for the web tier, On-Demand Instances for the application tier, and Reserved Instances for the database tier.
B. Use On-Demand Instances for the web and application tiers, and Reserved Instances for the database tier.
C. Use Spot Instances for the web and application tiers, and Reserved Instances for the database tier.
D. Use Reserved Instances for the web, application, and database tiers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 400
A company uses Amazon S3 to store documents that may only be accessible to an Amazon EC2 instance in a certain virtual private cloud (VPC). The company fears that a malicious insider with access to this instance could also set up an EC2 instance in another VPC to access these documents.

Which of the following solutions will provide the required protection?

A. Use an S3 VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint.
B. Use EC2 instance profiles and an S3 bucket policy to limit access to the role attached to the instance profile.
C. Use S3 client-side encryption and store the key in the instance metadata.
D. Use S3 server-side encryption and protect the key with an encryption context.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 401
The Solutions Architect manages a serverless application that consists of multiple API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables. Customers say that a few application components slow while loading dynamic images, and some are timing out with the "504 Gateway Timeout" error. While troubleshooting the scenario, the Solutions Architect confirms that DynamoDB monitoring metrics are at acceptable levels. Which of the following steps would be optimal for debugging these application issues? (Choose two.)

A. Parse HTTP logs in Amazon API Gateway for HTTP errors to determine the root cause of the errors.
B. Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals.
C. Parse VPC Flow Logs to determine if there is packet loss between the Lambda function and S3.
D. Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors.
E. Parse S3 access logs to determine if objects being accessed are from specific IP addresses to narrow the scope to geographic latency issues.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 402
A Solutions Architect is designing the storage layer for a recently purchased application. The application will be running on Amazon EC2 instances and has the following layers and requirements: ▪
Data layer: A POSIX file system shared across many systems.
▪ Service layer: Static file content that requires block storage with more than 100k IOPS.

Which combination of AWS services will meet these needs? (Choose two.)

A. Data layer – Amazon S3
B. Data layer – Amazon EC2 Ephemeral Storage
C. Data layer – Amazon EFS
D. Service layer – Amazon EBS volumes with Provisioned IOPS
E. Service layer – Amazon EC2 Ephemeral Storage

Correct Answer: AD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 403
A company has an application that runs a web service on Amazon EC2 instances and stores .jpg images in Amazon S3. The web traffic has a predictable baseline, but often demand spikes unpredictably for short periods of time. The application is loosely coupled and stateless. The .jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days, they are seldom accessed thereafter but always need to be immediately available. The CIO has asked to find ways to reduce costs.

Which of the following options will reduce costs? (Choose two.)

A. Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes.
B. Configure a lifecycle policy to move the .jpg images on Amazon S3 to S3 IA after 30 days.
C. Use On-Demand instances for baseline capacity requirements and use Spot Fleet instances for the demand spikes.
D. Configure a lifecycle policy to move the .jpg images on Amazon S3 to Amazon Glacier after 30 days.
E. Create a script that checks the load on all web servers and terminates unnecessary On-Demand instances.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 404
A hybrid network architecture must be used during a company's multi-year data center migration from multiple private data centers to AWS. The current data centers are linked together with private fiber. Due to unique legacy applications, NAT cannot be used. During the migration period, many applications will need access to other applications in both the data centers and AWS.

Which option offers a hybrid network architecture that is secure and highly available, that allows for high bandwidth and a multi-region deployment post-migration?

A. Use AWS Direct Connect to each data center from different ISPs, and configure routing to failover to the other data center's Direct Connect if one fails. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.
B. Use multiple hardware VPN connections to AWS from the on-premises data center. Route different subnet traffic through different VPN connections. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.
C. Use a software VPN with clustering both in AWS and the on-premises data center, and route traffic through the cluster. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.
D. Use AWS Direct Connect and a VPN as backup, and configure both to use the same virtual private gateway and BGP. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405
A company is currently running a production workload on AWS that is very I/O intensive. Its workload consists of a single tier with 10 c4.8xlarge instances, each with 2 TB gp2 volumes. The number of processing jobs has recently increased, and latency has increased as well. The team realizes that they are constrained on the IOPS. For the application to perform efficiently, they need to increase the IOPS by 3,000 for each of the instances.

Which of the following designs will meet the performance goal MOST cost effectively?

A. Change the type of Amazon EBS volume from gp2 to io1 and set provisioned IOPS to 9,000.
B. Increase the size of the gp2 volumes in each instance to 3 TB.
C. Create a new Amazon EFS file system and move all the data to this new file system. Mount this file system to all 10 instances.
D. Create a new Amazon S3 bucket and move all the data to this new bucket. Allow each instance to access this S3 bucket and use it for storage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 406
A company's data center is connected to the AWS Cloud over a minimally used 10-Gbps AWS Direct Connect connection with a private virtual interface to its virtual private cloud (VPC). The company internet connection is 200 Mbps, and the company has a 150-TB dataset that is created each Friday. The data must be transferred and available in Amazon S3 on Monday morning.

Which is the LEAST expensive way to meet the requirements while allowing for data transfer growth?

A. Order two 80-GB AWS Snowball appliances. Offload the data to the appliances and ship them to AWS. AWS will copy the data from the Snowball appliances to Amazon S3.
B. Create a VPC endpoint for Amazon S3. Copy the data to Amazon S3 by using the VPC endpoint, forcing the transfer to use the Direct Connect connection.
C. Create a VPC endpoint for Amazon S3. Set up a reverse proxy farm behind a Classic Load Balancer in the VPC. Copy the data to Amazon S3 using the proxy.
D. Create a public virtual interface on a Direct Connect connection, and copy the data to Amazon S3 over the connection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 407

A company has created an account for individual Development teams, resulting in a total of 200 accounts. All accounts have a single virtual private cloud (VPC) in a single region with multiple microservices running in Docker containers that need to communicate with microservices in other accounts. The Security team requirements state that these microservices must not traverse the public internet, and only certain internal services should be allowed to call other individual services. If there is any denied network traffic for a service, the Security team must be notified of any denied requests, including the source IP.

How can connectivity be established between service while meeting the security requirements?

A. Create a VPC peering connection between the VPCs. Use security groups on the instances to allow traffic from the security group IDs that are permitted to call the microservice. Apply network ACLs to and allow traffic from the localVPC and peered VPCs only. Within the task definition in Amazon ECS for each of the microservices, specify a log configuration by using the awslogs driver. Within Amazon CloudWatch Logs, create a metric filter and alarm off of the number of HTTP 403 responses. Create an alarm when the number of messages exceeds a threshold set by the Security team.

B. Ensure that no CIDR ranges are overlapping, and attach a virtual private gateway (VGW) to each VPC. Provision an IPsec tunnel between each VGW and enable route propagation on the route table. Configure security groups on eachservice to allow the CIDR ranges of the VPCs on the other accounts. Enable VPC Flow Logs, and use an Amazon CloudWatch Logs subscription filter for rejected traffic. Create an IAM role and allow the Security team to call the `AssumeRole` action for each account.

C. Deploy a transit VPC by using third-party marketplace VPN appliances running on Amazon EC2, dynamically routed VPN connections between the VPN appliance, and the virtual private gateways (VGWs) attached to each VPC withinthe region. Adjust network ACLs to allow traffic from the local VPC only. Apply security groups to the microservices to allow traffic from the VPN appliances only. Install the `awslogs` agent on each VPN appliance, and configure logs to forward to Amazon CloudWatch Logs in the security account for the Security team to access.

D. Create a Network Load Balancer (NLB) for each microservice. Attach the NLB to a PrivateLink endpoint service and whitelist the accounts that will be consuming this service. Create an interface endpoint in the consumer VPC andassociate a security group that allows only the security group IDs of the services authorized to call the producer service. On the producer services, create security groups for each microservice and allow only the CIDR range the allowed services. Create VPC Flow Logs on each VPC to capture rejected traffic that will be delivered to an Amazon CloudWatch Logs group. Create a CloudWatch Logs subscription that streams the log data to a security account.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 408

A company runs a dynamic mission-critical web application that has an SLA of 99.99%. Global application users access the application 24/7. The application is currently hosted on premises and routinely fails to meet its SLA, especially when millions of users access the application concurrently. Remote users complain of latency.

How should this application be redesigned to be scalable and allow for automatic failover at the lowest cost?

A. Use Amazon Route 53 failover routing with geolocation-based routing. Host the websiteon automatically scaled Amazon EC2 instances behind an Application Load Balancer with an additional Application Load Balancer and EC2instances for the application layer in each region. Use a Multi-AZ deployment with MySQL as the data layer.

B. Use Amazon Route 53 round robin routing to distribute the load evenly to several regions with health checks. Host the website on automatically scaled Amazon ECS with AWS Fargate technology containers behind a Network LoadBalancer, with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora replicas for the data layer.

C. Use Amazon Route 53 latency-based routing to route to the nearest region with health checks. Host the website in Amazon S3 in each region and use Amazon API Gateway with AWS Lambda for the application layer. Use AmazonDynamoDB global tables as the data layer with Amazon DynamoDB Accelerator (DAX) for caching.

D. Use Amazon Route 53 geolocation-based routing. Host the website on automatically scaled AWS Fargate containers behind a Network Load Balancer with an additional Network Load Balancer and Fargate containers for the applicationlayer in each region. Use Amazon Aurora Multi-Master for Aurora MySQL as the data layer.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 409

A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in a single AWS Region The fully qualified domain names (FQDNs) of all of the applications are made available through HTTPS using Application Load Balancers (ALBs). The ALBs are configured to use public SSL/TLS certificates.

A Solutions Architect needs to migrate the web applications to a multi-region architecture. All HTTPS services should continue to work without interruption.

Which approach meets these requirements?

A. Request a certificate for each FQDN using AWS KMS. Associate the certificates with the ALBs in the primary AWS Region. Enable cross-region availability in AWS KMS for the certificates and associate the certificates with the ALBs inthe secondary AWS Region.

B. Generate the key pairs and certificate requests for each FQDN using AWS KMS. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.

C. Request a certificate for each FQDN using AWS Certificate Manager. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
D. Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manager. Associate the certificates with the corresponding ALBs in each AWS Region.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 410
An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a Solutions Architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays.

Which of the following is the MOST reliable approach to meet the requirements?

A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
B. Receive the orders in an Amazon SQS queue and trigger an AWS Lambda function to process them.
C. Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container to process them.
D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 411
A company has an application written using an in-house software framework. The framework installation takes 30 minutes and is performed with a user data script. Company Developers deploy changes to the application frequently. The framework installation is becoming a bottleneck in this process.

Which of the following would speed up this process?

A. Create a pipeline to build a custom AMI with the framework installed and use this AMI as a baseline for application deployments.
B. Employ a user data script to install the framework but compress the installation files to make them smaller.
C. Create a pipeline to parallelize the installation tasks and call this pipeline from a user data script.
D. Configure an AWS OpsWorks cookbook that installs the framework instead of employing user data. Use this cookbook as a base for all deployments.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 412
A company wants to ensure that the workloads for each of its business units have complete autonomy and a minimal blast radius in AWS. The Security team must be able to control access to the resources and services in the account to ensure that particular services are not used by the business units.

How can a Solutions Architect achieve the isolation requirements?

A. Create individual accounts for each business unit and add the account to an OU in AWS Organizations. Modify the OU to ensure that the particular services are blocked. Federate each account with an IdP, and create separate roles forthe business units and the Security team.
B. Create individual accounts for each business unit. Federate each account with an IdP and create separate roles and policies for business units and the Security team.
C. Create one shared account for the entire company. Create separate VPCs for each business unit. Create individual IAM policies and resource tags for each business unit. Federate each account with an IdP, and create separate roles forthe business units and the Security team.
D. Create one shared account for the entire company. Create individual IAM policies and resource tags for each business unit. Federate the account with an IdP, and create separate roles for the business units and the Security team.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 413
A company is migrating a subset of its application APIs from Amazon EC2 instances to run on a serverless infrastructure. The company has set up Amazon API Gateway, AWS Lambda, and Amazon DynamoDB for the new application. The primary responsibility of the Lambda function is to obtain data from a third-party Software as a Service (SaaS) provider. For consistency, the Lambda function is attached to the same virtual private cloud (VPC) as the original EC2 instances.

Test users report an inability to use this newly moved functionality, and the company is receiving 5xx errors from API Gateway. Monitoring reports from the SaaS provider shows that the requests never made it to its systems. The company notices that Amazon CloudWatch Logs are being generated by the Lambda functions. When the same functionality is tested against the EC2 systems, it works as expected.

What is causing the issue?

A. Lambda is in a subnet that does not have a NAT gateway attached to it to connect to the SaaS provider.
B. The end-user application is misconfigured to continue using the endpoint backed by EC2 instances.
C. The throttle limit set on API Gateway is too low and the requests are not making their way through.
D. API Gateway does not have the necessary permissions to invoke Lambda.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414
A Solutions Architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month.

Which combination of steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Choose three.)

A. Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances.
B. Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types.
C. Purchase all upfront Reserved Instances that cover 100% of the account's expected Amazon EC2 usage.
D. Place conditions in the users' IAM policies that limit the number of instances they are able to launch.
E. Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console.
F. Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost.

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415
A large global company wants to migrate a stateless mission-critical application to AWS. The application is based on IBM WebSphere (application and integration middleware), IBM MQ (messaging middleware), and IBM DB2 (database software) on a z/OS operating system.

How should the Solutions Architect migrate the application to AWS?

A. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM MQ to an Amazon EC2-based MQ. Re-platform the z/OS-based DB2 to Amazon RDS DB2.
B. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM MQ to an Amazon MQ. Re-platform z/OS-based DB2 to Amazon EC2-based DB2.
C. Orchestrate and deploy the application by using AWS Elastic Beanstalk. Re-platform the IBM MQ to Amazon SQS. Re-platform z/OS-based DB2 to Amazon RDS DB2.
D. Use the AWS Server Migration Service to migrate the IBM WebSphere and IBM DB2 to an Amazon EC2-based solution. Re-platform the IBM MQ to an Amazon MQ.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 416

A media storage application uploads user photos to Amazon S3 for processing. End users are reporting that some uploaded photos are not being processed properly. The Application Developers trace the logs and find that AWS Lambda is experiencing execution issues when thousands of users are on the system simultaneously. Issues are caused by:

- Limits around concurrent executions.
- The performance of Amazon DynamoDB when saving data.

Which actions can be taken to increase the performance and reliability of the application? (Choose two.)

A. Evaluate and adjust the read capacity units (RCUs) for the DynamoDB tables.
B. Evaluate and adjust the write capacity units (WCUs) for the DynamoDB tables.
C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.
D. Configure a dead letter queue that will reprocess failed or timed-out Lambda functions.
E. Use S3 Transfer Acceleration to provide lower-latency access to end users.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 417

A company operates a group of imaging satellites. The satellites stream data to one of the company's ground stations where processing creates about 5 GB of images per minute. This data is added to network-attached storage, where 2 PB of data are already stored.

The company runs a website that allows its customers to access and purchase the images over the Internet. This website is also running in the ground station. Usage analysis shows that customers are most likely to access images that have been captured in the last 24 hours.

The company would like to migrate the image storage and distribution system to AWS to reduce costs and increase the number of customers that can be served.

Which AWS architecture and migration strategy will meet these requirements?

A. Use multiple AWS Snowball appliances to migrate the existing imagery to Amazon S3. Create a 1-Gb AWS Direct Connect connection from the ground station to AWS, and upload new data to Amazon S3 through the Direct Connectconnection. Migrate the data distribution website to Amazon EC2 instances. By using Amazon S3 as an origin, have this website serve the data through Amazon CloudFront by creating signed URLs.
B. Create a 1-Gb Direct Connect connection from the ground station to AWS. Use the AWS Command Line Interface to copy the existing data and upload new data to Amazon S3 over the Direct Connect connection. Migrate the datadistribution website to EC2 instances. By using Amazon S3 as an origin, have this website serve the data through CloudFront by creating signed URLs.
C. Use multiple Snowball appliances to migrate the existing images to Amazon S3. Upload new data by regularly using Snowball appliances to upload data from the network-attached storage. Migrate the data distribution website to EC2instances. By using Amazon S3 as an origin, have this website serve the data through CloudFront by creating signed URLs.
D. Use multiple Snowball appliances to migrate the existing images to an Amazon EFS file system. Create a 1-Gb Direct Connect connection from the ground station to AWS, and upload new data by mounting the EFS file system over theDirect Connect connection. Migrate the data distribution website to EC2 instances. By using webservers in EC2 that mount the EFS file system as the origin, have this website serve the data through CloudFront by creating signed URLs.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418

A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics is run, and each execution takes about 4 hours to complete. The statistical analysis is not mission critical to the business, and previous data points are picked up on the next execution if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations running full time to ingest and store the streaming data in attached Amazon EBS volumes. On-Demand EC2 instances are launched each night to perform the nightly processing, accessing the stored data from NFS shares on the ingestion servers, and terminating the nightly processing servers when complete. The Reserved Instance reservations are expiring, and the company needs to determine whether to purchase new reservations or implement a new design.

Which is the most cost-effective design?

A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a fleet of On-Demand EC2 instances that launches each night to perform the batch processing of the S3 data and terminates when theprocessing completes.
B. Update the ingestion process to use Amazon Kinesis Data Firehouse to save data to Amazon S3. Use AWS Batch to perform nightly processing with a Spot market bid of 50% of the On-Demand price.
C. Update the ingestion process to use a fleet of EC2 Reserved Instances behind a Network Load Balancer with 3-year leases. Use Batch with Spot instances with a maximum bid of 50% of the On-Demand price for the nightly processing.D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use an AWS Lambda function scheduled to run nightly with Amazon CloudWatch Events to query Amazon Redshift to generate the daily statistics.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 419
A three-tier web application runs on Amazon EC2 instances. Cron daemons are used to trigger scripts that collect the web server, application, and database logs and send them to a centralized location every hour. Occasionally, scaling events or unplanned outages have caused the instances to stop before the latest logs were collected, and the log files were lost.

Which of the following options is the MOST reliable way of collecting and preserving the log files?

A. Update the cron to run every 5 minutes instead of every hour to reduce the possibility of log messages being lost in an outage.
B. Use Amazon CloudWatch Events to trigger Amazon Systems Manager Run Command to invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage.
C. Use the Amazon CloudWatch Logs agent to stream log messages directly to CloudWatch Logs. Configure the agent with a batch count of 1 to reduce the possibility of log messages being lost in an outage.
D. Use Amazon CloudWatch Events to trigger AWS Lambda to SSH into each running instance and invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 420
A company stores sales transaction data in Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes to the items stored in the DynamoDB tables must be logged within 30 minutes.

Which solution meets the requirements?

A. Copy the DynamoDB tables into Apache Hive tables on Amazon EMR every hour and analyze them for anomalous behaviors. Send Amazon SNS notifications when anomalous behaviors are detected.
B. Use AWS CloudTrail to capture all the APIs that change the DynamoDB tables. Send SNS notifications when anomalous behaviors are detected using CloudTrail event filtering.
C. Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda. Create a Lambda function to output records to Amazon Kinesis Data Streams. Analyze any anomalies with Amazon Kinesis Data Analytics. Send SNSnotifications when anomalous behaviors are detected.
D. Use event patterns in Amazon CloudWatch Events to capture DynamoDB API call events with an AWS Lambda function as a target to analyze behavior. Send SNS notifications when anomalous behaviors are detected.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 421
A company is running multiple applications on Amazon EC2. Each application is deployed and managed by multiple business units. All applications are deployed on a single AWS account but on different virtual private clouds (VPCs). The company uses a separate VPC in the same account for test and development purposes.

Production applications suffered multiple outages when users accidentally terminated and modified resources that belonged to another business unit. A Solutions Architect has been asked to improve the availability of the company applications while allowing the Developers access to the resources they need.

Which option meets the requirements with the LEAST disruption?

A. Create an AWS account for each business unit. Move each business unit's instances to its own account and set up a federation to allow users to access their business unit's account.
B. Set up a federation to allow users to use their corporate credentials, and lock the users down to their own VPC. Use a network ACL to block each VPC from accessing other VPCs.
C. Implement a tagging policy based on business units. Create an IAM policy so that each user can terminate instances belonging to their own business units only.
D. Set up role-based access for each user and provide limited permissions based on individual roles and the services for which each user is responsible.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 422
An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP, Java, or Ruby web applications, are no longer actively developed, and serve little traffic.

Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs?

A. Deploy the applications to single-instance AWS Elastic Beanstalk environments without a load balancer.
B. Use AWS SMS to create AMIs for each virtual machine and run them in Amazon EC2.
C. Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.
D. Use VM Import/Export to create AMIs for each virtual machine and run them in single-instance AWS Elastic Beanstalk environments by configuring a custom image.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423
A Solutions Architect must create a cost-effective backup solution for a company's 500MB source code repository of proprietary and sensitive applications. The repository runs on Linux and backs up daily to tape. Tape backups are stored for 1 year.
The current solutions are not meeting the company's needs because it is a manual process that is prone to error, expensive to maintain, and does not meet the need for a Recovery Point Objective (RPO) of 1 hour or Recovery Time Objective (RTO) of 2 hours. The new disaster recovery requirement is for backups to be stored offsite and to be able to restore a single file if needed.

Which solution meets the customer's needs for RTO, RPO, and disaster recovery with the LEAST effort and expense?

A. Replace local tapes with an AWS Storage Gateway virtual tape library to integrate with current backup software. Run backups nightly and store the virtual tapes on Amazon S3 standard storage in US-EAST-1. Use cross-regionreplication to create a second copy in US-WEST-2. Use Amazon S3 lifecycle policies to perform automatic migration to Amazon Glacier and deletion of expired backups after 1 year?
B. Configure the local source code repository to synchronize files to an AWS Storage Gateway file Amazon gateway to store backup copies in an Amazon S3 Standard bucket. Enable versioning on the Amazon S3 bucket. Create AmazonS3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard 0 Infrequent Access, then Amazon Glacier, then delete backups after 1 year.
C. Replace the local source code repository storage with a Storage Gateway stored volume. Change the default snapshot frequency to 1 hour. Use Amazon S3 lifecycle policies to archive snapshots to Amazon Glacier and remove oldsnapshots after 1 year. Use cross-region replication to create a copy of the snapshots in US-WEST-2.
D. Replace the local source code repository storage with a Storage Gateway cached volume. Create a snapshot schedule to take hourly snapshots. Use an Amazon CloudWatch Events schedule expression rule to run on hourly AWSLambda task to copy snapshots from US-EAST -1 to US-WEST-2.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424

A company CFO recently analyzed the company's AWS monthly bill and identified an opportunity to reduce the cost for AWS Elastic Beanstalk environments in use. The CFO has asked a Solutions Architect to design a highly available solution that will spin up an Elastic Beanstalk environment in the morning and terminate it at the end of the day.

The solution should be designed with minimal operational overhead and to minimize costs. It should also be able to handle the increased use of Elastic Beanstalk environments among different teams, and must provide a one-stop scheduler solution for all teams to keep the operational costs low.

What design will meet these requirements?

A. Set up a Linux EC2 Micro instance. Configure an IAM role to allow the start and stop of the Elastic Beanstalk environment and attach it to the instance. Create scripts on the instance to start and stop the Elastic Beanstalk environment.Configure cron jobs on the instance to execute the scripts.
B. Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution role granting Elastic Beanstalk environment start/stop permissions, and assign the role to the Lambda functions.Configure cron expression Amazon CloudWatch Events rules to trigger the Lambda functions.
C. Develop an AWS Step Functions state machine with "wait" as its type to control the start and stop time. Use the activity task to start and stop the Elastic Beanstalk environment. Create a role for Step Functions to allow it to start and stopthe Elastic Beanstalk environment. Invoke Step Functions daily.
D. Configure a time-based Auto Scaling group. In the morning, have the Auto Scaling group scale up an Amazon EC2 instance and put the Elastic Beanstalk environment `start` command in the EC2 instance user date. At the end of the day, scale down the instance number to 0 to terminate the EC2 instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 425
A company plans to move regulated and security-sensitive businesses to AWS. The Security team is developing a framework to validate the adoption of AWS best practice and industry-recognized compliance standards. The AWS Management Console is the preferred method for teams to provision resources.

Which strategies should a Solutions Architect use to meet the business requirements and continuously assess, audit, and monitor the configurations of AWS resources? (Choose two.)

A. Use AWS Config rules to periodically audit changes to AWS resources and monitor the compliance of the configuration. Develop AWS Config custom rules using AWS Lambda to establish a test-driven development approach, andfurther automate the evaluation of configuration changes against the required controls.
B. Use Amazon CloudWatch Logs agent to collect all the AWS SDK logs. Search the log data using a pre-defined set of filter patterns that machines mutating API calls. Send notifications using Amazon CloudWatch alarms whenunintended changes are performed. Archive log data by using a batch export to Amazon S3 and then Amazon Glacier for a long-term retention and auditability.
C. Use AWS CloudTrail events to assess management activities of all AWS accounts. Ensure that CloudTrail is enabled in all accounts and available AWS services. Enable trails, encrypt CloudTrail event log files with an AWS KMS key,and monitor recorded activities with CloudWatch Logs.
D. Use the Amazon CloudWatch Events near-real-time capabilities to monitor system events patterns, and trigger AWS Lambda functions to automatically revert non-authorized changes in AWS resources. Also, target Amazon SNS topicsto enable notifications and improve the response time of incident responses.
E. Use CloudTrail integration with Amazon SNS to automatically notify unauthorized API activities. Ensure that CloudTrail is enabled in all accounts and available AWS services. Evaluate the usage of Lambda functions to automaticallyrevert non-authorized changes in AWS resources.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426
A company is running a high-user-volume media-sharing application on premises. It currently hosts about 400 TB of data with millions of video files. The company is migrating this application to AWS to improve reliability and reduce costs.

The Solutions Architecture team plans to store the videos in an Amazon S3 bucket and use Amazon CloudFront to distribute videos to users. The company needs to migrate this application to AWS 10 days with the least amount of downtime possible. The company currently has 1 Gbps connectivity to the Internet with 30 percent free capacity.

Which of the following solutions would enable the company to migrate the workload to AWS and meet all of the requirements?

A. Use a multi-part upload in Amazon S3 client to parallel-upload the data to the Amazon S3 bucket over the Internet. Use the throttling feature to ensure that the Amazon S3 client does not use more than 30 percent of available Internetcapacity.

B. Request an AWS Snowmobile with 1 PB capacity to be delivered to the data center. Load the data into Snowmobile and send it back to have AWS download that data to the Amazon S3 bucket. Sync the new data that was generatedwhile migration was in flight.

C. Use an Amazon S3 client to transfer data from the data center to the Amazon S3 bucket over the Internet. Use the throttling feature to ensure the Amazon S3 client does not use more than 30 percent of available Internet capacity.D. Request multiple AWS Snowball devices to be delivered to the data center. Load the data concurrently into these devices and send it back. Have AWS download that data to the Amazon S3 bucket. Sync the new data that was generated while migration was in flight.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 427
A company has developed a new billing application that will be released in two weeks. Developers are testing the application running on 10 EC2 instances managed by an Auto Scaling group in subnet 172.31.0.0/24 within VPC A with CIDR block 172.31.0.0/16. The Developers noticed connection timeout errors in the application logs while connecting to an Oracle database running on an Amazon EC2 instance in the same region within VPC B with CIDR block 172.50.0.0/16. The IP of the database instance is hard-coded in the application instances.

Which recommendations should a Solutions Architect present to the Developers to solve the problem in a secure way with minimal maintenance and overhead?

A. Disable the SrcDestCheck attribute for all instances running the application and Oracle Database. Change the default route of VPC A to point ENI of the Oracle Database that has an IP address assigned within the range of 172.50.0.0/26
B. Create and attach internet gateways for both VPCs. Configure default routes to the Internet gateways for both VPCs. Assign an Elastic IP for each Amazon EC2 instance in VPC A
C. Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 172.50.0.0/16
D. Create an additional Amazon EC2 instance for each VPC as a customer gateway; create one virtual private gateway (VGW) for each VPC, configure an end-to-end VPC, and advertise the routes for 172.50.0.0/16

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 428
A Solutions Architect has been asked to look at a company's Amazon Redshift cluster, which has quickly become an integral part of its technology and supports key business process. The Solutions Architect is to increase the reliability and availability of the cluster and provide options to ensure that if an issue arises, the cluster can either operate or be restored within four hours.

Which of the following solution options BEST addresses the business need in the most cost-effective manner?

A. Ensure that the Amazon Redshift cluster has been set up to make use of Auto Scaling groups with the nodes in the cluster spread across multiple Availability Zones.
B. Ensure that the Amazon Redshift cluster creation has been template using AWS CloudFormation so it can easily be launched in another Availability Zone and data populated from the automated Redshift back-ups stored in Amazon S3.
C. Use Amazon Kinesis Data Firehose to collect the data ahead of ingestion into Amazon Redshift and create clusters using AWS CloudFormation in another region and stream the data to both clusters.
D. Create two identical Amazon Redshift clusters in different regions (one as the primary, one as the secondary). Use Amazon S3 cross-region replication from the primary to secondary). Use Amazon S3 cross-region replication from theprimary to secondary region, which triggers an AWS Lambda function to populate the cluster in the secondary region.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 429
A company prefers to limit running Amazon EC2 instances to those that were launched from AMIs pre-approved by the Information Security department. The Development team has an agile continuous integration and deployment process that cannot be stalled by the solution.

Which method enforces the required controls with the LEAST impact on the development process? (Choose two.)

A. Use IAM policies to restrict the ability of users or other automated entities to launch EC2 instances based on a specific set of pre-approved AMIs, such as those tagged in a specific way by Information Security.

B. Use regular scans within Amazon Inspector with a custom assessment template to determine if the EC2 instance that the Amazon Inspector Agent is running on is based upon a pre-approved AMI. If it is not, shut down the instance andinform information Security by email that this occurred.
C. Only allow launching of EC2 instances using a centralized DevOps team, which is given work packages via notifications from an internal ticketing system. Users make requests for resources using this ticketing tool, which has manualinformation security approval steps to ensure that EC2 instances are only launched from approved AMIs.
D. Use AWS Config rules to spot any launches of EC2 instances based on non-approved AMIs, trigger an AWS Lambda function to automatically terminate the instance, and publish a message to an Amazon SNS topic to informInformation Security that this occurred.
E. Use a scheduled AWS Lambda function to scan through the list of running instances within the virtual private cloud (VPC) and determine if any of these are based on unapproved AMIs. Publish a message to an SNS topic to informInformation Security that this occurred and then shut down the instance.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 430
A Company has a security event whereby an Amazon S3 bucket with sensitive information was made public. Company policy is to never have public S3 objects, and the Compliance team must be informed immediately when any public objects are identified.

How can the presence of a public S3 object be detected, set to trigger alarm notifications, and automatically remediated in the future? (Choose two.)

A. Turn on object-level logging for Amazon S3. Turn on Amazon S3 event notifications to notify by using an Amazon SNS topic when a PutObject API call is made with a public-read permission.
B. Configure an Amazon CloudWatch Events rule that invokes an AWS Lambda function to secure the S3 bucket.
C. Use the S3 bucket permissions for AWS Trusted Advisor and configure a CloudWatch event to notify by using Amazon SNS.
D. Turn on object-level logging for Amazon S3. Configure a CloudWatch event to notify by using an SNS topic when a PutObject API call with public-read permission is detected in the AWS CloudTrail logs.
E. Schedule a recursive Lambda function to regularly change all object permissions inside the S3 bucket.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
A company is using an Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer. The web application requires user authorization and session tracking for dynamic content. The CloudFront distribution has a single cache behavior configured to forward the Authorization, Host, and User-Agent HTTP whitelist headers and a session cookie to the origin. All other cache behavior settings are set to their default value.

A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings. The ACM certificate is also applied to the HTTPS listener for the Application Load Balancer. The CloudFront origin protocol policy is set to HTTPS only. Analysis of the cache statistics report shows that the miss rate for this distribution is very high.

What can the Solutions Architect do to improve the cache hit rate for this distribution without causing the SSL/TLS handshake between CloudFront and the Application Load Balancer to fail?

A. Create two cache behaviors for static and dynamic content. Remove the User-Agent and `Host` HTTP headers from the whitelist headers section on both if the cache behaviors. Remove the session cookie from the whitelist cookies section and the `Authorization` HTTP header from the whitelist headers section for cache behavior configured for static content.
B. Remove the `User-Agent` and `Authorization` HTTPS headers from the whitelist headers section of the cache behavior. Then update the cache behavior to use presigned cookies for authorization.
C. Remove the `Host` HTTP header from the whitelist headers section and remove the session cookie from the whitelist cookies section for the default cache behavior. Enable automatic object compression and use Lambda@Edge viewer request events for user authorization.
D. Create two cache behaviors for static and dynamic content. Remove the `User-Agent` HTTP header from the whitelist headers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the `Authorization` HTTP header from the whitelist headers section for cache behavior configured for static content.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 432

An organization has a write-intensive mobile application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The application has scaled well, however, costs have increased exponentially because of higher than anticipated Lambda costs. The application's use is unpredictable, but there has been a steady 20% increase in utilization every month.

While monitoring the current Lambda functions, the Solutions Architect notices that the execution-time averages 4.5 minutes. Most of the wait time is the result of a high-latency network call to a 3-TB MySQL database server that is onpremises. A VPN is used to connect to the VPC, so the Lambda functions have been configured with a five-minute timeout.

How can the Solutions Architect reduce the cost of the current architecture?

A. ▪ Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database.
▪ Enable local caching in the mobile application to reduce the Lambda function invocation calls.
▪ Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time. ▪ Offload
the frequently accessed records from DynamoDB to Amazon ElastiCache.

B. ▪ Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database.
▪ Cache the API Gateway results to Amazon CloudFront.
▪ Use Amazon EC2 Reserved Instances instead of Lambda.
▪ Enable Auto Scaling on EC2, and use Spot Instances during peak times. ▪
Enable DynamoDB Auto Scaling to manage target utilization.

C. ▪ Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.
▪ Enable caching of the Amazon API Gateway results in Amazon CloudFront to reduce the number of Lambda function invocations.
▪ Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.
▪ Enable DynamoDB Accelerator for frequently accessed records, and enable the DynamoDB Auto Scaling feature.

D. ▪ Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.
▪ Enable API caching on API Gateway to reduce the number of Lambda function invocations.
▪ Continue to monitor the AWS Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time. ▪ Enable
Auto Scaling in DynamoDB.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433

A company runs a video processing platform. Files are uploaded by users who connect to a web server, which stores them on an Amazon EFS share. This web server is running on a single Amazon EC2 instance. A different group of instances, running in an Auto Scaling group, scans the EFS share directory structure for new files to process and generates new videos (thumbnails, different resolution, compression, etc.) according to the instructions file, which is uploaded along with the video files. A different application running on a group of instances managed by an Auto Scaling group processes the video files and then deletes them from the EFS share. The results are stored in an S3 bucket. Links to the processed video files are emailed to the customer.

The company has recently discovered that as they add more instances to the Auto Scaling Group, many files are processed twice, so image processing speed is not improved. The maximum size of these video files is 2GB.
What should the Solutions Architect do to improve reliability and reduce the redundant processing of video files?

A. Modify the web application to upload the video files directly to Amazon S3. Use Amazon CloudWatch Events to trigger an AWS Lambda function every time a file is uploaded, and have this Lambda function put a message into anAmazon queue for new files and use the queue depth metric to scale instances in the video processing Auto Scaling group.

B. Set up a cron job on the web server instance to synchronize the contents of the EFS share into Amazon S3. Trigger an AWS Lambda function every time a file is uploaded to process the video file and store the results in Amazon S3.Using Amazon CloudWatch Events trigger an Amazon SES job to send an email to the customer containing the link to the processed file.

C. Rewrite the web application to run directly from Amazon S3 and use Amazon API Gateway to upload the video files to an S3 bucket. Use an S3 trigger to run an AWS Lambda function each time a file is uploaded to process and storenew video files in a different bucket. Using CloudWatch Events, trigger an SES job to send an email to the customer containing the link to the processed file.

D. Rewrite the application to run from Amazon S3 and upload the video files to an S3 bucket. Each time a new file is uploaded, trigger an AWS Lambda function to put a message in an SQS queue containing the link and the instructions.Modify the video processing application to read from the SQS queue and the S3 bucket. Use the queue depth metric to adjust the size of the Auto Scaling group for video processing instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 434 A Solutions Architect must establish a patching plan for a large mixed fleet of Windows and Linux servers. The patching plan must be implemented securely, be audit ready, and comply with the company's business requirements.

Which option will meet these requirements with MINIMAL effort?

A. Install and use an OS-native patching service to manage the update frequency and release approval for all instances. Use AWS Config to verify the OS state on each instance and report on any patch compliance issues.
B. Use AWS Systems Manager on all instances to manage patching. Test patches outside of production and then deploy during a maintenance window with the appropriate approval.
C. Use AWS OpsWorks for Chef Automate to run a set of scripts that will iterate through all instances of a given type. Issue the appropriate OS command to get and install updates on each instance, including any required restarts duringthe maintenance window.
D. Migrate all applications to AWS OpsWorks and use OpsWorks automatic patching support to keep the OS up-to-date following the initial installation. Use AWS Config to provide audit and compliance reporting.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 435
A Solutions Architect must design a highly available, stateless, REST service. The service will require multiple persistent storage layers for service object meta information and the delivery of content. Each request needs to be authenticated and securely processed. There is a requirement to keep costs as low as possible?

How can these requirements be met?

A. Use AWS Fargate to host a container that runs a self-contained REST service. Set up an Amazon ECS service that is fronted by an Application Load Balancer (ALB). Use a custom authenticator to control access to the API. Storerequest meta information in Amazon DynamoDB with Auto Scaling and static content in a secured S3 bucket. Make secure signed requests for Amazon S3 objects and proxy the data through the REST service interface.
B. Use AWS Fargate to host a container that runs a self-contained REST service. Set up an ECS service that is fronted by a cross-zone ALB. Use an Amazon Cognito user pool to control access to the API. Store request meta informationin DynamoDB with Auto Scaling and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.
C. Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon Cognito user pool to control access to the API. Configure the methods to use AWS Lambda proxy integrations, and process eachresource with a unique AWS Lambda function. Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.
D. Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon API Gateway custom authorizer to control access to the API. Configure the methods to use AWS Lambda custom integrations, andprocess each resource with a unique Lambda function. Store request meta information in an Amazon ElastiCache Multi-AZ cluster and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 436
A large company experienced a drastic increase in its monthly AWS spend. This is after Developers accidentally launched Amazon EC2 instances in unexpected regions. The company has established practices around least privileges for Developers and controls access to on-premises resources using Active Directory groups. The company now want to control costs by restricting the level of access that Developers have to the AWS Management Console without impacting their productivity. The company would also like to allow Developers to launch Amazon EC2 in only one region, without limiting access to other services in any region.

How can this company achieve these new security requirements while minimizing the administrative burden on the Operations team?

A. Set up SAML-based authentication tied to an IAM role that has an AdministrativeAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.
B. Create an IAM user for each Developer and add them to the developer IAM group that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that allows the Developers access to Amazon EC2 onlyin the required region.
C. Set up SAML-based authentication tied to an IAM role that has a PowerUserAccess managed policy and a customer managed policy that deny all the Developers access to any AWS services except AWS Service Catalog. Within AWSService Catalog, create a product containing only the EC2 resources in the approved region.
D. Set up SAML-based authentication tied to an IAM role that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 437

A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier.

Company policy requires IT to durably store nightly backups f all its data in at least two locations: production and disaster recovery. The locations must be in different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location. All backup processes must be fully automated.

What is the MOST cost-effective backup solution that will meet all requirements?

A. Back up all the data to a large Amazon EBS volume attached to the backup media server in the production region. Run automated scripts to snapshot these volumes nightly, and copy these snapshots to the disaster recovery region.
B. Back up all the data to Amazon S3 in the disaster recovery region. Use a lifecycle policy to move this data to Amazon Glacier in the production region immediately. Only the data is replicated; remove the data from the S3 bucket in thedisaster recovery region.
C. Back up all the data to Amazon Glacier in the production region. Set up cross-region replication of this data to Amazon Glacier in the disaster recovery region. Set up a lifecycle policy to delete any data older than 60 days.
D. Back up all the data to Amazon S3 in the production region. Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438

A company has an existing on-premises three-tier web application. The Linux web servers serve content from a centralized file share on a NAS server because the content is refreshed several times a day from various sources. The existing infrastructure is not optimized and the company would like to move to AWS in order to gain the ability to scale resources up and down in response to load. On-premises and AWS resources are connected using AWS Direct Connect.

How can the company migrate the web infrastructure to AWS without delaying the content refresh process?

A. Create a cluster of web server Amazon EC2 instances behind a Classic Load Balancer on AWS. Share an Amazon EBS volume among all instances for the content. Schedule a periodic synchronization of this volume and the NASserver.
B. Create an on-premises file gateway using AWS Storage Gateway to replace the NAS server and replicate content to AWS. On the AWS side, mount the same Storage Gateway bucket to each web server Amazon EC2 instance to servethe content.
C. Expose an Amazon EFS share to on-premises users to serve as the NAS serve. Mount the same EFS share to the web server Amazon EC2 instances to serve the content.
D. Create web server Amazon EC2 instances on AWS in an Auto Scaling group. Configure a nightly process where the web server instances are updated from the NAS server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 439

A company has multiple AWS accounts hosting IT applications. An Amazon CloudWatch Logs agent is installed on all Amazon EC2 instances. The company wants to aggregate all security events in a centralized AWS account dedicated to log storage.

Security Administrators need to perform near-real-time gathering and correlating of events across multiple AWS accounts.

Which solution satisfies these requirements?

A. Create a Log Audit IAM role in each application AWS account with permissions to view CloudWatch Logs, configure an AWS Lambda function to assume the Log Audit role, and perform an hourly export of CloudWatch Logs data to anAmazon S3 bucket in the logging AWS account.
B. Configure CloudWatch Logs streams in each application AWS account to forward events to CloudWatch Logs in the logging AWS account. In the logging AWS account, subscribe an Amazon Kinesis Data Firehose stream to AmazonCloudWatch Events, and use the stream to persist log data in Amazon S3.
C. Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to CloudWatch Logs streams in each application AWS account, configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams asits source, and persist the log data in an Amazon S3 bucket inside the logging AWS account.
D. Configure CloudWatch Logs agents to publish data to an Amazon Kinesis Data Firehose stream in the logging AWS account, use an AWS Lambda function to read messages from the stream and push messages to Data Firehose, andpersist the data in Amazon S3.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 440
A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified.

How can this be accomplished?

A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function. For changes to Lambda, create an AWSCloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
B. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code. Rollback if Amazon CloudWatch alarms aretriggered.
C. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version.
D. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected,change the AWS CloudFront origin to the previous API Gateway endpoint.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 441
A company is running a .NET three-tier web application on AWS. The team currently uses XL storage optimized instances to store serve the website's image and video files on local instance storage. The company has encountered issues with data loss from replication and instance failures. The Solutions Architect has been asked to redesign this application to improve its reliability while keeping costs low.

Which solution will meet these requirements?

A. Set up a new Amazon EFS share, move all image and video files to this share, and then attach this new drive as a mount point to all existing servers. Create an Elastic Load Balancer with Auto Scaling general purpose instances. EnableAmazon CloudFront to the Elastic Load Balancer. Enable Cost Explorer and use AWS Trusted advisor checks to continue monitoring the environment for future savings.
B. Implement Auto Scaling with general purpose instance types and an Elastic Load Balancer. Enable an Amazon CloudFront distribution to Amazon S3 and move images and video files to Amazon S3. Reserve general purpose instancesto meet base performance requirements. Use Cost Explorer and AWS Trusted Advisor checks to continue monitoring the environment for future savings.
C. Move the entire website to Amazon S3 using the S3 website hosting feature. Remove all the web servers and have Amazon S3 communicate directly with the application servers in Amazon VPC.
D. Use AWS Elastic Beanstalk to deploy the .NET application. Move all images and video files to Amazon EFS. Create an Amazon CloudFront distribution that points to the EFS share. Reserve the m4.4xl instances needed to meet baseperformance requirements.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 442
A company has developed a web application that runs on Amazon EC2 instances in one AWS Region. The company has taken on new business in other countries and must deploy its application into other to meet low-latency requirements for its users. The regions can be segregated, and an application running in one region does not need to communicate with instances in other regions.

How should the company's Solutions Architect automate the deployment of the application so that it can be MOST efficiently deployed into multiple regions?

A. Write a bash script that uses the AWS CLI to query the current state in one region and output a JSON representation. Pass the JSON representation to the AWS CLI, specifying the `--region` parameter to deploy the application to other regions.

B. Write a bash script that uses the AWS CLI to query the current state in one region and output an AWS CloudFormation template. Create a CloudFormation stack from the template by using the AWS CLI, specifying the `--region` parameter to deploy the application to other regions.
C. Write a CloudFormation template describing the application's infrastructure in the resources section. Create a CloudFormation stack from the template by using the AWS CLI, specify multiple regions using the `--regions` parameter to deploy the application.
D. Write a CloudFormation template describing the application's infrastructure in the Resources section. Use a CloudFormation stack set from an administrator account to launch stack instances that deploy the application to other regions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 443
A media company has a 30-TB repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.

The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system.

How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

A. Set up an AWS Storage Gateway, file gateway appliance on premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway. Use the catalog of faces to build a collection in AmazonRekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.
B. Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway. Use the catalog of faces to build a collection in AmazonRekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution.
C. Configure a video ingestion stream by using Amazon Kinesis Video Streams. Use the catalog of faces to build a collection in Amazon Rekognition. Stream the videos from the MAM solution into Kinesis Video Streams. ConfigureAmazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3.
D. Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the one-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve therequired metadata, and push the metadata into the MAM solution while also copying the video files to an Amazon S3 bucket.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 444
A company is planning the migration of several lab environments used for software testing. An assortment of custom tooling is used to manage the test runs for each lab. The labs use immutable infrastructure for the software test runs, and the results are stored in a highly available SQL database cluster. Although completely rewriting the custom tooling is out of scope for the migration project, the company would like to optimize workloads during the migration.

Which application migration strategy meets this requirement?

A. Re-host
B. Re-platform
C. Re-factor/re-architect
D. Retire

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 445
A company is implementing a multi-account strategy; however, the Management team has expressed concerns that services like DNS may become overly complex. The company needs a solution that allows private DNS to be shared among virtual private clouds (VPCs) in different accounts. The company will have approximately 50 accounts in total.

What solution would create the LEAST complex DNS architecture and ensure that each VPC can resolve all AWS resources?

A. Create a shared services VPC in a central account, and create a VPC peering connection from the shared services VPC to each of the VPCs in the other accounts. Within Amazon Route 53, create a privately hosted zone in the sharedservices VPC and resource record sets for the domain and subdomains. Programmatically associate other VPCs with the hosted zone.
B. Create a VPC peering connection among the VPCs in all accounts. Set the VPC attributes enableDnsHostnames and enableDnsSupport to “true” for each VPC. Create an Amazon Route 53 private zone for each VPC. Create resourcerecord sets for the domain and subdomains. Programmatically associate the hosted zones in each VPC with the other VPCs.
C. Create a shared services VPC in a central account. Create a VPC peering connection from the VPCs in other accounts to the shared services VPC. Create an Amazon Route 53 privately hosted zone in the shared services VPC withresource record sets for the domain and subdomains. Allow UDP and TCP port 53 over the VPC peering connections.
D. Set the VPC attributes enableDnsHostnames and enableDnsSupport to “false” in every VPC. Create an AWS Direct Connect connection with a private virtual interface. Allow UDP and TCP port 53 over the virtual interface. Use the on-premises DNS servers to resolve the IP addresses in each VPC on AWS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 446
A company has asked a Solutions Architect to design a secure content management solution that can be accessed by API calls by external customer applications. The company requires that a customer administrator must be able to submit an API call and roll back changes to existing files sent to the content management solution, as needed.

What is the MOST secure deployment design that meets all solution requirements?

A. Use Amazon S3 for object storage with versioning and bucket access logging enabled, and an IAM role and access policy for each customer application. Encrypt objects using SSE-KMS. Develop the content management application touse a separate AWS KMS key for each customer.
B. Use Amazon WorkDocs for object storage. Leverage WorkDocs encryption, user access management, and version control. Use AWS CloudTrail to log all SDK actions and create reports of hourly access by using the AmazonCloudWatch dashboard. Enable a revert function in the SDK based on a static Amazon S3 webpage that shows the output of the CloudWatch dashboard.
C. Use Amazon EFS for object storage, using encryption at rest for the Amazon EFS volume and a customer managed key stored in AWS KMS. Use IAM roles and Amazon EFS access policies to specify separate encryption keys for eachcustomer application. Deploy the content management application to store all new versions as new files in Amazon EFS and use a control API to revert a specific file to a previous version.
D. Use Amazon S3 for object storage with versioning and enable S3 bucket access logging. Use an IAM role and access policy for each customer application. Encrypt objects using client-side encryption, and distribute an encryption key toall customers when accessing the content management application.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 447
A company has released a new version of a website to target an audience in Asia and South America. The website’s media assets are hosted on Amazon S3 and have an Amazon CloudFront distribution to improve end-user performance. However, users are having a poor login experience the authentication service is only available in the us-east-1 AWS Region.

How can the Solutions Architect improve the login experience and maintain high security and performance with minimal management overhead?

A. Replicate the setup in each new geography and use Amazon Route 53 geo-based routing to route traffic to the AWS Region closest to the users.
B. Use an Amazon Route 53 weighted routing policy to route traffic to the CloudFront distribution. Use CloudFront cached HTTP methods to improve the user login experience.
C. Use Amazon Lambda@Edge attached to the CloudFront viewer request trigger to authenticate and authorize users by maintaining a secure cookie token with a session expiry to improve the user experience in multiple geographies.
D. Replicate the setup in each geography and use Network Load Balancers to route traffic to the authentication service running in the closest region to users.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 448

A company has a standard three-tier architecture using two Availability Zones. During the company's off season, users report that the website is not working. The Solutions Architect finds that no changes have been made to the environment recently, the website is reachable, and it is possible to log in. However, when the Solutions Architect selects the "find a store near you" function, the maps provided on the site by a third-party RESTful API call do not work about 50% of the time after refreshing the page. The outbound API calls are made through Amazon EC2 NAT instances.

What is the MOST likely reason for this failure and how can it be mitigated in the future?

A. The network ACL for one subnet is blocking outbound web traffic. Open the network ACL and prevent administration from making future changes through IAM.
B. The fault is in the third-party environment. Contact the third party that provides the maps and request a fix that will provide better uptime.
C. One NAT instance has become overloaded. Replace both EC2 NAT instances with a larger-sized instance and make sure to account for growth when making the new instance size.
D. One of the NAT instances failed. Recommend replacing the EC2 NAT instances with a NAT gateway.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449
A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.

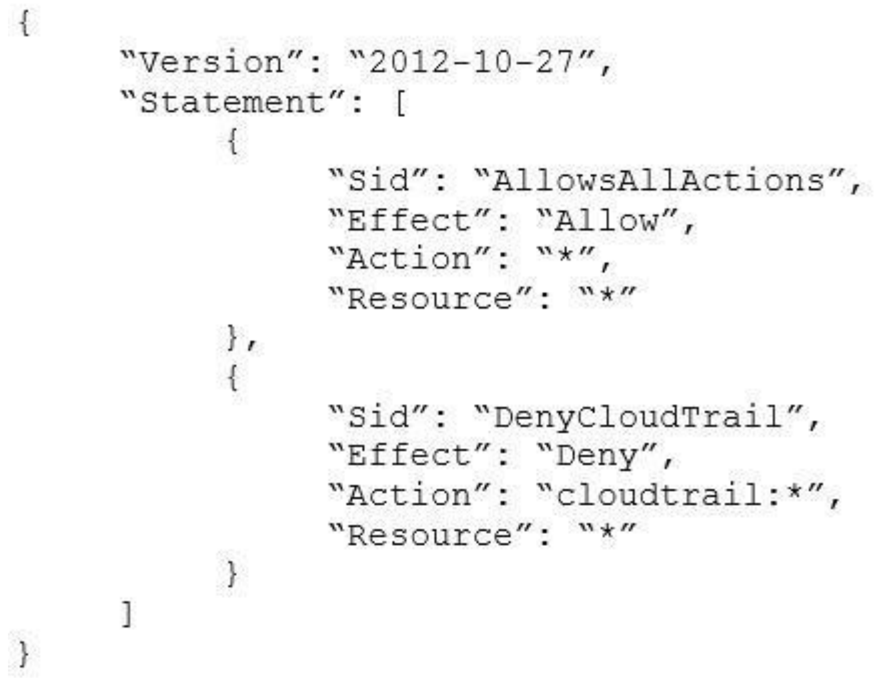
Which would enable the collection of this data MOST cost effectively?

A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.
B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.
C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.
D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 450
A company will several AWS accounts is using AWS Organizations and service control policies (SCPs). An Administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-11111111:



```
{
      "Version": "2012-10-27",
      "Statement": [
            {
                  "Sid": "AllowsAllActions",
                  "Effect": "Allow",
                  "Action": "*",
                  "Resource": "*"
            },
            {
                  "Sid": "DenyCloudTrail",
                  "Effect": "Deny",
                  "Action": "cloudtrail:*",
                  "Resource": "*"
            }
      ]
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the Administrator address this problem?

A. Add `s3:CreateBucket` with "Allow" effect to the SCP.
B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
C. Instruct the Developers to add Amazon S3 permissions to their IAM entities.
D. Remove the SCP from account 1111-1111-1111.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 451
A company that provides wireless services needs a solution to store and analyze log files about user activities. Currently, log files are delivered daily to Amazon Linux on Amazon EC2 instance. A batch script is run once a day to aggregate data used for analysis by a third-party tool. The data pushed to the third-party tool is used to generate a visualization for end users. The batch script is cumbersome to maintain, and it takes several hours to deliver the ever-increasing data volumes to the third-party tool. The company wants to lower costs, and is open to considering a new tool that minimizes development effort and lowers administrative overhead. The company wants to build a more agile solution that can store and perform the analysis in near-real time, with minimal overhead. The solution needs to be cost effective and scalable to meet the company's end-user base growth.

Which solution meets the company's requirements?

A. Develop a Python script to failure the data from Amazon EC2 in real time and store the data in Amazon S3. Use a `copy` command to copy data from Amazon S3 to Amazon Redshift. Connect a business intelligence tool running on Amazon EC2 to Amazon Redshift and create the visualizations.
B. Use an Amazon Kinesis agent running on an EC2 instance in an Auto Scaling group to collect and send the data to an Amazon Kinesis Data Forehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the datadirectly to Amazon ES. Use Kibana to visualize the data.
C. Use an in-memory caching application running on an Amazon EBS-optimized EC2 instance to capture the log data in near real-time. Install an Amazon ES cluster on the same EC2 instance to store the log files as they are delivered toAmazon EC2 in near real-time. Install a Kibana plugin to create the visualizations.
D. Use an Amazon Kinesis agent running on an EC2 instance to collect and send the data to an Amazon Kinesis Data Firehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data to Amazon S3. Use an AWSLambda function to deliver the data from Amazon S3 to Amazon ES. Use Kibana to visualize the data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 452
A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.

Which service will meet the requirements for storing the session information in the MOST cost-effective way?

A. Amazon ElastiCache with the Memcached engine
B. Amazon S3
C. Amazon RDS MySQL
D. Amazon ElastiCache with the Redis engine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference https://aws.amazon.com/caching/session-management/

QUESTION 453
A company has an Amazon EC2 deployment that has the following architecture:
- An application tier that contains 8 m4.xlarge instances
- A Classic Load Balancer
- Amazon S3 as a persistent data store

After one of the EC2 instances fails, users report very slow processing of their requests. A Solutions Architect must recommend design changes to maximize system reliability. The solution must minimize costs.

What should the Solution Architect recommend?

A. Migrate the existing EC2 instances to a serverless deployment using AWS Lambda functions
B. Change the Classic Load Balancer to an Application Load Balancer
C. Replace the application tier with m4.large instances in an Auto Scaling groupD. Replace the application tier with 4 m4.2xlarge instances

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 454
An on-premises application will be migrated to the cloud. The application consists of a single Elasticsearch virtual machine with data source feeds from local systems that will not be migrated, and a Java web application on Apache Tomcat running on three virtual machines. The Elasticsearch server currently uses 1 TB of storage out of 16 TB available storage, and the web application is updated every 4 months. Multiple users access the web application from the Internet. There is a 10Gbit AWS Direct Connect connection established, and the application can be migrated over a schedules 48-hour change window.

Which strategy will have the LEAST impact on the Operations staff after the migration?

A. Create an Elasticsearch server on Amazon EC2 right-sized with 2 TB of Amazon EBS and a public AWS Elastic Beanstalk environment for the web application. Pause the data sources, export the Elasticsearch index from on premises,and import into the EC2 Elasticsearch server. Move data source feeds to the new Elasticsearch server and move users to the web application.
B. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Use AWS DMS to replicate Elasticsearch data. When replication has finished, move data source feeds to the newAmazon ES cluster endpoint and move users to the new web application.
C. Use the AWS SMS to replicate the virtual machines into AWS. When the migration is complete, pause the data source feeds and start the migrated Elasticsearch and web application instances. Place the web application instancesbehind a public Elastic Load Balancer. Move the data source feeds to the new Elasticsearch server and move users to the new web Application Load Balancer.
D. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Pause the data source feeds, export the Elasticsearch index from on premises, and import into the Amazon EScluster. Move the data source feeds to the new Amazon ES cluster endpoint and move users to the new web application.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 455

A company's application is increasingly popular and experiencing latency because of high volume reads on the database server.

The service has the following properties:
▪ A highly available REST API hosted in one region using Application Load Balancer (ALB) with auto scaling. ▪
A MySQL database hosted on an Amazon EC2 instance in a single Availability Zone.

The company wants to reduce latency, increase in-region database read performance, and have multi-region disaster recovery capabilities that can perform a live recovery automatically without any data or performance loss (HA/DR).

Which deployment strategy will meet these requirements?

A. Use AWS CloudFormation StackSets to deploy the API layer in two regions. Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region and a read replica in a different region thanthe source database cluster. Use Amazon Route 53 health checks to trigger a DNS failover to the standby region if the health checks to the primary load balancer fail. In the event of Route 53 failover, promote the cross-region database replica to be the master and build out new read replicas in the standby region.
B. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. In the event of failure,use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.
C. Use AWS CloudFormation StackSets to deploy the API layer in two regions. Add the database to an Auto Scaling group. Add a read replica to the database in the second region. Use Amazon Route 53 health checks in the primaryregion fail. Promote the cross-region database replica to be the master and build out new read replicas in the standby region.
D. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. Use Amazon Route 53health checks on the ALB to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 456

A company runs a three-tier application in AWS. Users report that the application performance can vary greatly depending on the time of day and functionality being accessed.

The application includes the following components:
▪ Eight t2.large front-end web servers that serve static content and proxy dynamic content from the application tier. ▪
Four t2.large application servers.
▪ One db.m4.large Amazon RDS MySQL Multi-AZ DB instance.

Operations has determined that the web and application tiers are network constrained.

Which of the following should cost effective improve application performance? (Choose two.)

A. Replace web and app tiers with t2.xlarge instances
B. Use AWS Auto Scaling and m4.large instances for the web and application tiers
C. Convert the MySQL RDS instance to a self-managed MySQL cluster on Amazon EC2
D. Create an Amazon CloudFront distribution to cache content
E. Increase the size of the Amazon RDS instance to db.m4.xlarge

Correct Answer: AC
Section: (none)
Explanation
Explanation/Reference:

QUESTION 457

An online retailer needs to regularly process large product catalogs, which are handled in batches. These are sent out to be processed by people using the Amazon Mechanical Turk service, but the retailer has asked its Solutions Architect to design a workflow orchestration system that allows it to handle multiple concurrent Mechanical Turk operations, deal with the result assessment process, and reprocess failures.

Which of the following options gives the retailer the ability to interrogate the state of every workflow with the LEAST amount of implementation effort?

A. Trigger Amazon CloudWatch alarms based upon message visibility in multiple Amazon SQS queues (one queue per workflow stage) and send messages via Amazon SNS to trigger AWS Lambda functions to process the next step. UseAmazon ES and Kibana to visualize Lambda processing logs to see the workflow states.
B. Hold workflow information in an Amazon RDS instance with AWS Lambda functions polling RDS for status changes. Worker Lambda functions then process the next workflow steps. Amazon QuickSight will visualize workflow statesdirectly out of Amazon RDS.
C. Build the workflow in AWS Step Functions, using it to orchestrate multiple concurrent workflows. The status of each workflow can be visualized in the AWS Management Console, and historical data can be written to Amazon S3 andvisualized using Amazon QuickSight.
D. Use Amazon SWF to create a workflow that handles a single batch of catalog records with multiple worker tasks to extract the data, transform it, and send it through Mechanical Turk. Use Amazon ES and Kibana to visualize AWSLambda processing logs to see the workflow states.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 458
An organization has two Amazon EC2 instances:
▪ The first is running an ordering application and an inventory application. ▪
The second is running a queuing system.

During certain times of the year, several thousand orders are placed per second. Some orders were lost when the queuing system was down. Also, the organization's inventory application has the incorrect quantity of products because some orders were processed twice.

What should be done to ensure that the applications can handle the increasing number of orders?

A. Put the ordering and inventory applications into their own AWS Lambda functions. Have the ordering application write the messages into an Amazon SQS FIFO queue.
B. Put the ordering and inventory applications into their own Amazon ECS containers and create an Auto Scaling group for each application. Then, deploy the message queuing server in multiple Availability Zones.
C. Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each application. Use Amazon SQS standard queues for the incoming orders, and implement idempotency in theinventory application.
D. Put the ordering and inventory applications into their own Amazon EC2 instances. Write the incoming orders to an Amazon Kinesis data stream Configure AWS Lambda to poll the stream and update the inventory application.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 459
A company is migrating its on-premises build artifact server to an AWS solution. The current system consists of an Apache HTTP server that serves artifacts to clients on the local network, restricted by the perimeter firewall. The artifact consumers are largely build automation scripts that download artifacts via anonymous HTTP, which the company will be unable to modify within its migration timetable.

The company decides to move the solution to Amazon S3 static website hosting. The artifact consumers will be migrated to Amazon EC2 instances located within both public and private subnets in a virtual private cloud (VPC).

Which solution will permit the artifact consumers to download artifacts without modifying the existing automation scripts?

A. Create a NAT gateway within a public subnet of the VPC. Add a default route pointing to the NAT gateway into the route table associated with the subnets containing consumers. Configure the bucket policy to allow the `s3:ListBucket` and `s3:GetObject` actions using the condition `IpAddress` and the condition key `aws:SourceIp` matching the elastic IP address if the NAT gateway.
B. Create a VPC endpoint and add it to the route table associated with subnets containing consumers. Configure the bucket policy to allow `s3:ListBucket` and `s3:GetObject` actions using the condition `StringEquals` and the condition key `aws:sourceVpce` matching the identification of the VPC endpoint.
C. Create an IAM role and instance profile for Amazon EC2 and attach it to the instances that consume build artifacts. Configure the bucket policy to allow the s3:ListBucket and s3:GetObjects actions for the principal matching the IAM rolecreated.

D. Create a VPC endpoint and add it to the route table associated with subnets containing consumers. Configure the bucket policy to allow `s3:ListBucket` and `s3:GetObject` actions using the condition `IpAddress` and the condition key `aws:SourceIp` matching the VPC CIDR block.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 460
A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs for requests and data transfers from Amazon S3.

Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers?

A. Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Have the organizations assumeand use that read role when accessing the data.
B. Ensure that all organizations in the partnership have AWS accounts. Create a bucket policy on the bucket that owns the data. The policy should allow the accounts in the partnership read access to the bucket. Enable Requester Pays onthe bucket. Have the organizations use their AWS credentials when accessing the data.
C. Ensure that all organizations in the partnership have AWS accounts. Configure buckets in each of the accounts with a bucket policy that allows the institute that owns the data the ability to write to the bucket. Periodically sync the datafrom the institute's account to the other organizations. Have the organizations use their AWS credentials when accessing the data using their accounts.
D. Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Enable Requester Pays on thebucket. Have the organizations assume and use that read role when accessing the data.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 461
A company currently uses a single 1 Gbps AWS Direct Connect connection to establish connectivity between an AWS Region and its data center. The company has five Amazon VPCs, all of which are connected to the data center using the same Direct Connect connection. The Network team is worried about the single point of failure and is interested in improving the redundancy of the connections to AWS while keeping costs to a minimum.

Which solution would improve the redundancy of the connection to AWS while meeting the cost requirements?

A. Provision another 1 Gbps Direct Connect connection and create new VIFs to each of the VPCs. Configure the VIFs in a load balancing fashion using BGP.
B. Set up VPN tunnels from the data center to each VPC. Terminate each VPN tunnel at the virtual private gateway (VGW) of the respective VPC and set up BGP for route management.
C. Set up a new point-to-point Multiprotocol Label Switching (MPLS) connection to the AWS Region that's being used. Configure BGP to use this new circuit as passive, so that no traffic flows through this unless the AWS Direct Connectfails.
D. Create a public VIF on the Direct Connect connection and set up a VPN tunnel which will terminate on the virtual private gateway (VGW) of the respective VPC using the public VIF. Use BGP to handle the failover to the VPNconnection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 462
A company currently uses Amazon EBS and Amazon RDS for storage purposes. The company intends to use a pilot light approach for disaster recovery in a different AWS Region. The company has an RTO of 6 hours and an RPO of 24 hours.
Which solution would achieve the requirements with MINIMAL cost?

A. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacityset to 0 in the disaster recovery region.

B. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group configured in thesame way as in the primary region.
C. Use Amazon ECS to handle long-running tasks to create daily EBS and RDS snapshots, and copy to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scalinggroup with the capacity set to 0 in the disaster recovery region.
D. Use EBS and RDS cross-region snapshot copy capability to create snapshots in the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacityset to 0 in the disaster recovery region.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 463
A company needs to cost-effectively persist small data records (up to 1 KiB) for up to 30 days. The data is read rarely. When reading the data, a 5-minute delay is acceptable.

Which of the following solutions achieve this goal? (Choose two.)

A. Use Amazon S3 to collect multiple records in one S3 object. Use a lifecycle configuration to move data to Amazon Glacier immediately after write. Use expedited retrievals when reading the data.
B. Write the records to Amazon Kinesis Data Firehose and configure Kinesis Data Firehose to deliver the data to Amazon S3 after 5 minutes. Set an expiration action at 30 days on the S3 bucket.
C. Use an AWS Lambda function invoked via Amazon API Gateway to collect data for 5 minutes. Write data to Amazon S3 just before the Lambda execution stops.
D. Write the records to Amazon DynamoDB configured with a Time To Live (TTL) of 30 days. Read data using the `GetItem` or `BatchGetItem` call.
E. Write the records to an Amazon ElastiCache for Redis. Configure the Redis append-only file (AOF) persistence logs to write to Amazon S3. Recover from the log if the ElastiCache instance has failed.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 464
A Development team is deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS Lambda, and Amazon DynamoDB resources. A Solutions Architect has been tasked with automating the future deployments of these serverless APIs.

How can this be accomplished?

A. Use AWS CloudFormation with a Lambda-backed custom resource to provision API Gateway. Use the AWS::DynamoDB::Table and AWS::Lambda::Function resources to create the Amazon DynamoDB table and Lambda functions.Write a script to automate the deployment of the CloudFormation template.
B. Use the AWS Serverless Application Model to define the resources. Upload a YAML template and application files to the code repository. Use AWS CodePipeline to connect to the code repository and to create an action to build usingAWS CodeBuild. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution.
C. Use AWS CloudFormation to define the serverless application. Implement versioning on the Lambda functions and create aliases to point to the versions. When deploying, configure weights to implement shifting traffic to the newestversion, and gradually update the weights as traffic moves over.
D. Commit the application code to the AWS CodeCommit code repository. Use AWS CodePipeline and connect to the CodeCommit code repository. Use AWS CodeBuild to build and deploy the Lambda functions using AWS CodeDeploy.Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 465
The company Security team queries that all data uploaded into an Amazon S3 bucket must be encrypted. The encryption keys must be highly available and the company must be able to control access on a per-user basis, with different users having access to different encryption keys.

Which of the following architectures will meet these requirements? (Choose two.)

A. Use Amazon S3 server-side encryption with Amazon S3-managed keys. Allow Amazon S3 to generate an AWS/S3 master key, and use IAM to control access to the data keys that are generated.
B. Use Amazon S3 server-side encryption with AWS KMS-managed keys, create multiple customer master keys, and use key policies to control access to them.
C. Use Amazon S3 server-side encryption with customer-managed keys, and use AWS CloudHSM to manage the keys. Use CloudHSM client software to control access to the keys that are generated.
D. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use the Cloud HSM client software to control access to the keysthat are generated.
E. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use IAM to control access to the keys that are generated inCloudHSM.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference http://jayendrapatil.com/tag/kms/

QUESTION 466
A company runs a public-facing application that uses a Java-based web service via a RESTful API. It is hosted on Apache Tomcat on a single server in a data center that runs consistently at 30% CPU utilization. Use of the API is expected to increase by 10 times with a new product launch. The business wants to migrate the application to AWS with no disruption, and needs it to scale to meet demand.

The company has already decided to use Amazon Route 53 and CNAME records to redirect traffic. How can these requirements be met with the LEAST amount of effort?

A. Use AWS Elastic Beanstalk to deploy the Java web service and enable Auto Scaling. Then switch the application to use the new web service.
B. Lift and shift the Apache server to the cloud using AWS SMS. Then switch the application to direct web service traffic to the new instance.
C. Create a Docker image and migrate the image to Amazon ECS. Then change the application code to direct web service queries to the ECS container.
D. Modify the application to call the web service via Amazon API Gateway. Then create a new AWS Lambda Java function to run the Java web service code. After testing, change API Gateway to use the Lambda function.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 467
A company is using AWS for production and development workloads. Each business unit has its own AWS account for production, and a separate AWS account to develop and deploy its applications. The Information Security department has introduced new security policies that limit access for terminating certain Amazon ECs instances in all accounts to a small group of individuals from the Security team.

How can the Solutions Architect meet these requirements?

A. Create a new IAM policy that allows access to those EC2 instances only for the Security team. Apply this policy to the AWS Organizations master account.
B. Create a new tag-based IAM policy that allows access to these EC2 instances only for the Security team. Tag the instances appropriately, and apply this policy in each account.
C. Create an organizational unit under AWS Organizations. Move all the accounts into this organizational unit and use SCP to apply a whitelist policy to allow access to these EC2 instances for the Security team only.
D. Set up SAML federation for all accounts in AWS. Configure SAML so that it checks for the service API call before authenticating the user. Block SAML from authenticating API calls if anyone other than the Security team accesses theseinstances.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 468
A company is moving a business-critical, multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A Solutions Architect must re-architect the application to ensure that it can meet or exceed the SLA.

The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application.

Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?

A. Migrate the database to a PostgreSQL database in Amazon EC2. Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Allocate an Amazon WorkSpacesWorkSpace for each end user to improve the user experience.
B. Migrate the database to an Amazon RDS Aurora PostgreSQL configuration. Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer. Use AmazonAppStream 2.0 to improve the user experience.
C. Migrate the database to an Amazon RDS PostgreSQL Multi-AZ configuration. Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balancer. Use Amazon ElastiCache toimprove the user experience.
D. Migrate the database to an Amazon Redshift cluster with at least two nodes. Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Use AmazonCloudFront to improve the user experience.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: