

AWS Certified Solutions Architect - Professional

Passing Score: 800
Time Limit: 120 min
File Version: 1

AWS Certified Solutions Architect - Professional

Exam A

QUESTION 1

You have recently joined a startup company building sensors to measure street noise and air quality in urban areas. The company has been running a pilot deployment of around 100 sensors for 3 months each sensor uploads 1KB of sensor data every minute to a backend hosted on AWS.

During the pilot, you measured a peak of 10 IOPS on the database, and you stored an average of 3GB of sensor data per month in the database.

The current deployment consists of a load-balanced auto scaled Ingestion layer using EC2 instances and a PostgreSQL RDS database with 500GB standard storage.

The pilot is considered a success and your CEO has managed to get the attention of some potential investors. The business plan requires a deployment of at least 100K sensors which needs to be supported by the backend. You also need to store sensor data for at least two years to be able to compare year over year Improvements.

To secure funding, you have to make sure that the platform meets these requirements and leaves room for further scaling.

Which setup will meet the requirements?

- A. Add an SQS queue to the ingestion layer to buffer writes to the RDS instance
- B. 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 2

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 all traffic across the VPC.
- B. Create a second VPC and route all traffic from the primary application VPC through the second VPC where the scalable virtualized IDS/IPS platform resides.
- C. Configure servers running in the VPC using the host-based 'route' commands to send all traffic through the platform to a scalable virtualized IDS/IPS.
- D. Configure each host with an agent that collects all network traffic and sends that traffic to the IDS/IPS platform for inspection.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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 three.)

- 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:

Reference:

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

QUESTION 4

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 5

You've been hired to enhance the overall security posture for a very large e-commerce site. They have a well architected multi-tier application running in a VPC that uses ELBs in front of both the web and the app tier with static assets served directly from S3. They are using a combination of RDS and DynamoDB for their dynamic data and then archiving nightly into S3 for further processing with EMR. They are concerned because they found questionable log entries and 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 then pass the traffic to the current web tier. The web tier Security Groups would be updated to only allow traffic from the WAF tier Security Group.
- D. Remove all but TLS 1.2 from the web tier ELB and enable Advanced Protocol Filtering. This will enable the ELB itself to perform WAF functionality.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

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 will 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 EMR with Amazon Kinesis and save the results to DynamoDB.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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 two.)

- 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 CNAME 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 8

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

The application currently consists of 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 traffic between on-premises web servers and those hosted in AWS.
- C. Offload traffic from on-premises environment: Setup a CloudFront 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 exist in 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 replica and setup replication between the RDS instance and on-premises MySQL server to migrate the database.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can have CloudFront sit in front of your on-prem web environment, via a custom origin (the origin doesn't have to be in AWS). This would protect against unexpected bursts in traffic by letting CloudFront handle the traffic that it can out of cache, thus hopefully removing some of the load from your on-prem web servers.

QUESTION 9

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:

Explanation:

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

QUESTION 10

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 of 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 in-memory cache horizontally than a relational database.

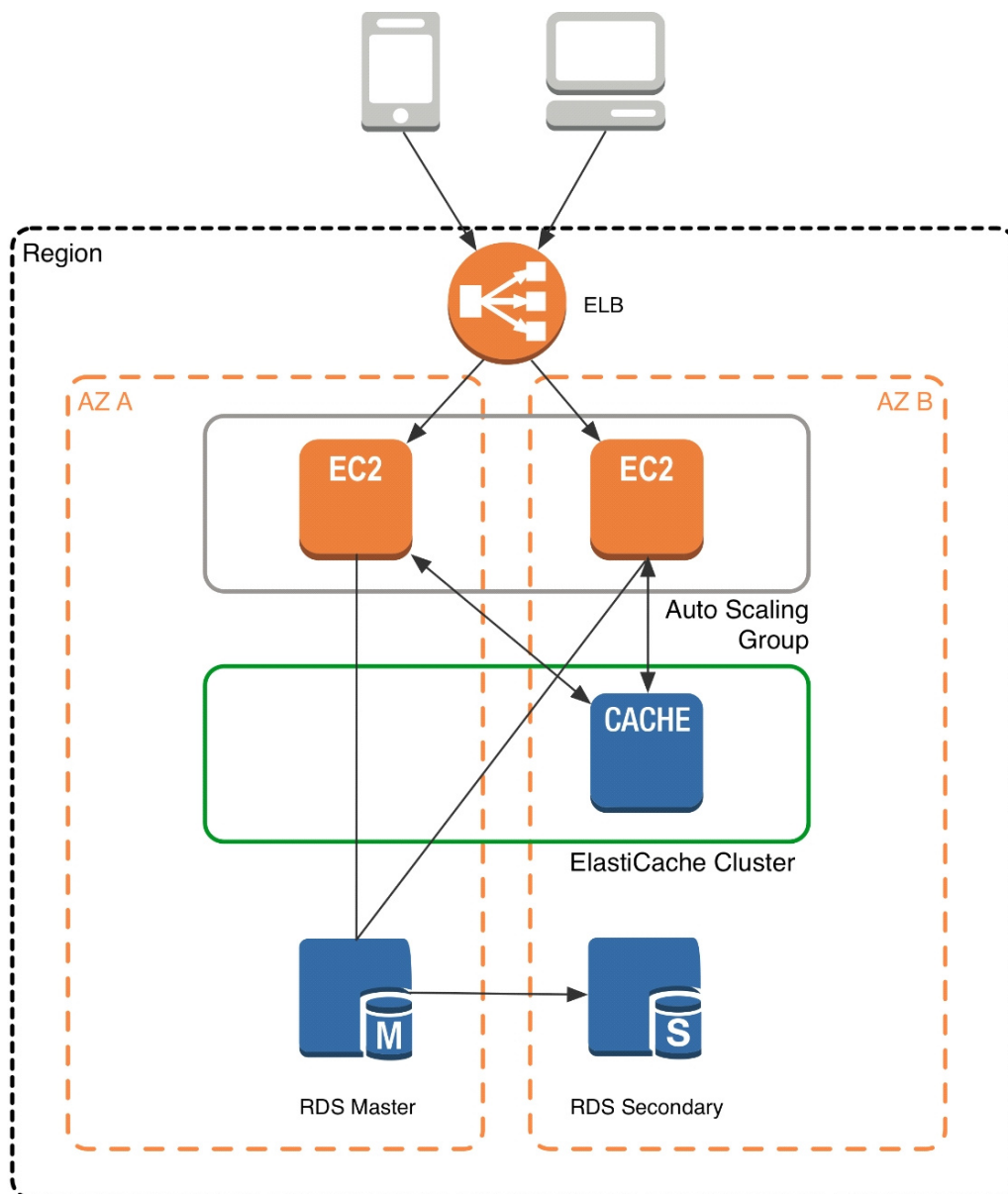
Last, a caching layer provides a request buffer in the event of a sudden spike in usage. If your app or game ends up on the front page of Reddit or the App Store, it's not unheard of to see a spike that is 10 to 100 times your normal application load. Even if you autoscale your application instances, 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 caching-focused solution.

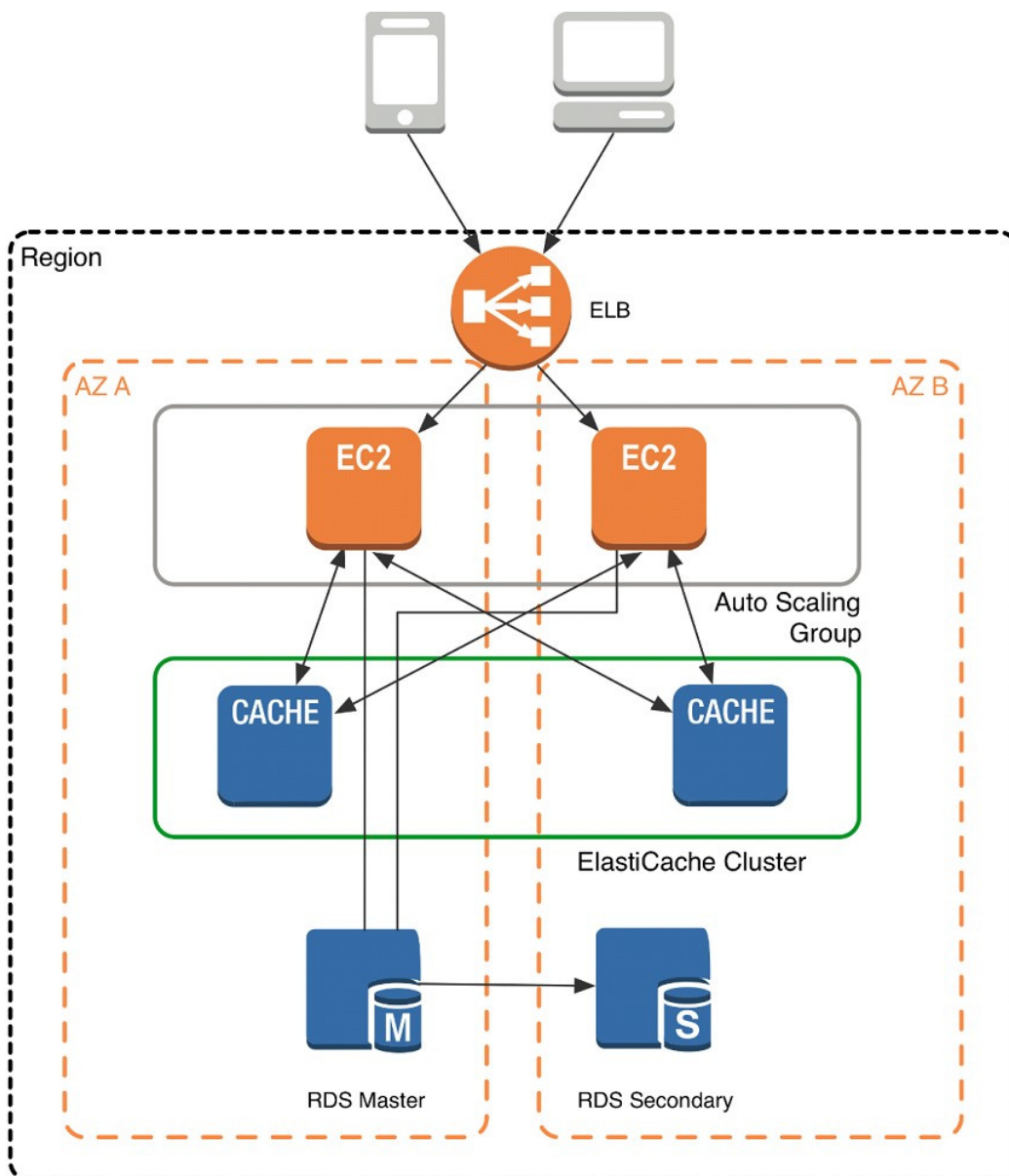
We'll revisit Redis later in the paper, and weigh its advantages and disadvantages.

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:

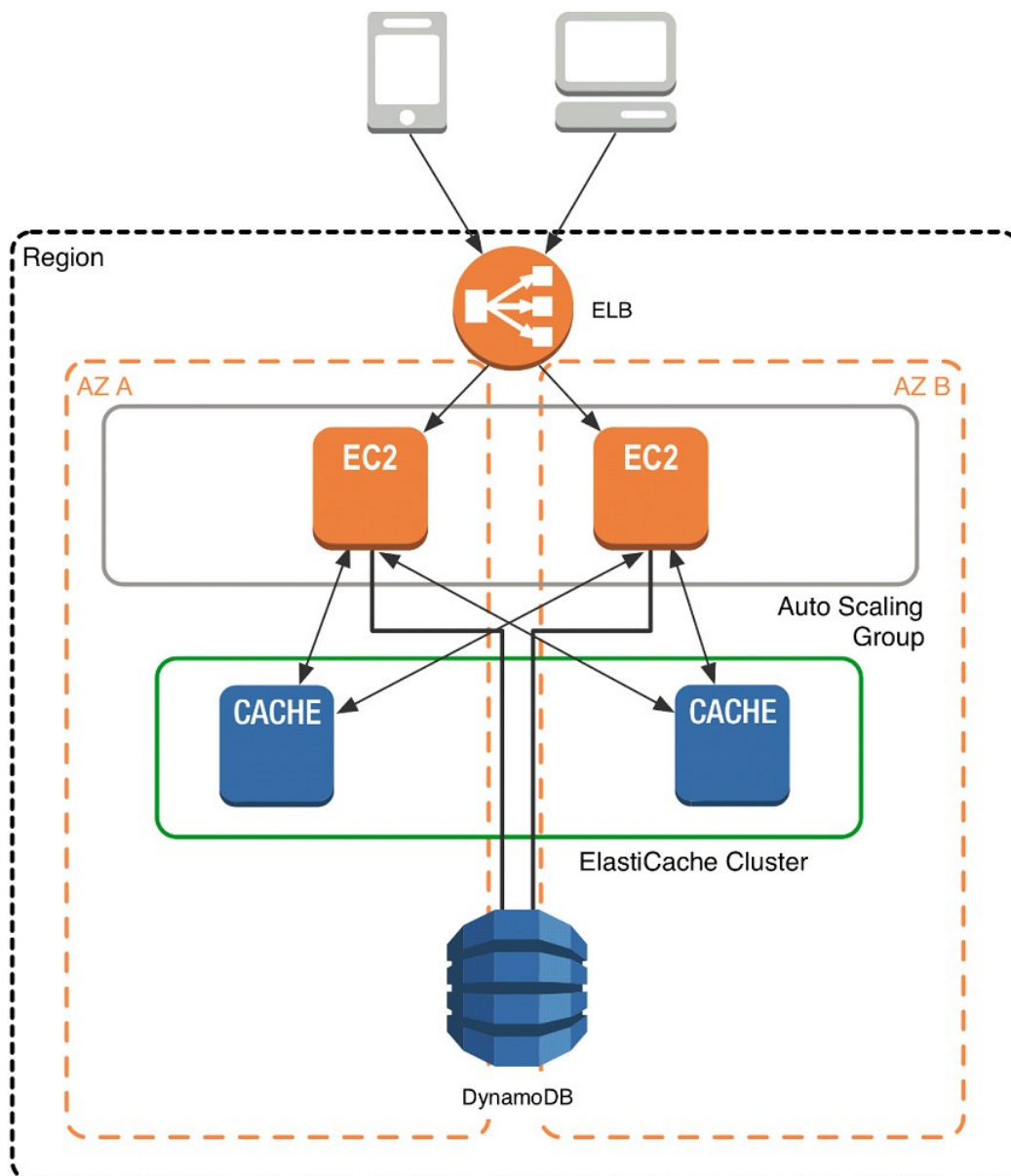


In this architecture diagram, the Amazon EC2 application instances are in an Auto Scaling group, located behind a load balancer using Elastic Load Balancing, which distributes requests among the instances. As requests come into a given EC2 instance, that EC2 instance is responsible for communicating 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 11

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: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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 13

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 14

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 15

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. Global
- C. Secure. Flexible. Cost-effective. Scalable and elastic. Experienced
- D. Flexible. Cost-effective. Dynamic. Secure. Experienced.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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 17

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 18

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 to store and serve the scanned files, install the commercial search application on EC2 Instances and configure with auto-scaling and an Elastic Load Balancer.
- B. Model the environment using CloudFormation use an EC2 instance running Apache webserver and an open source search application, stripe multiple standard EBS volumes together to store the JPEGs and search index.
- C. Use S3 with standard redundancy to store and serve the scanned files, use CloudSearch for query processing, and use Elastic Beanstalk to host the website across multiple availability zones.
- D. Use a single-AZ RDS MySQL instance to store the search index and 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 for 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+ELBs 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 its 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, JPEG2000 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 I can't comment on that. Regardless of which option, I'd use CloudFormation for all of it.

QUESTION 19

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-compliant 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:

Reference:

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

QUESTION 20

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 21

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 then 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 RDS 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 22

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 autoscaling 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 23

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's memory 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:

Explanation:

We can use either RDS or DynamoDB, however in our given answers, IAM role is mentioned only with RDS, so I would go with Answer B. Question was explicitly focused on security, so IAM with RDS is the best choice.

QUESTION 24

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 two.)

- 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 25

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

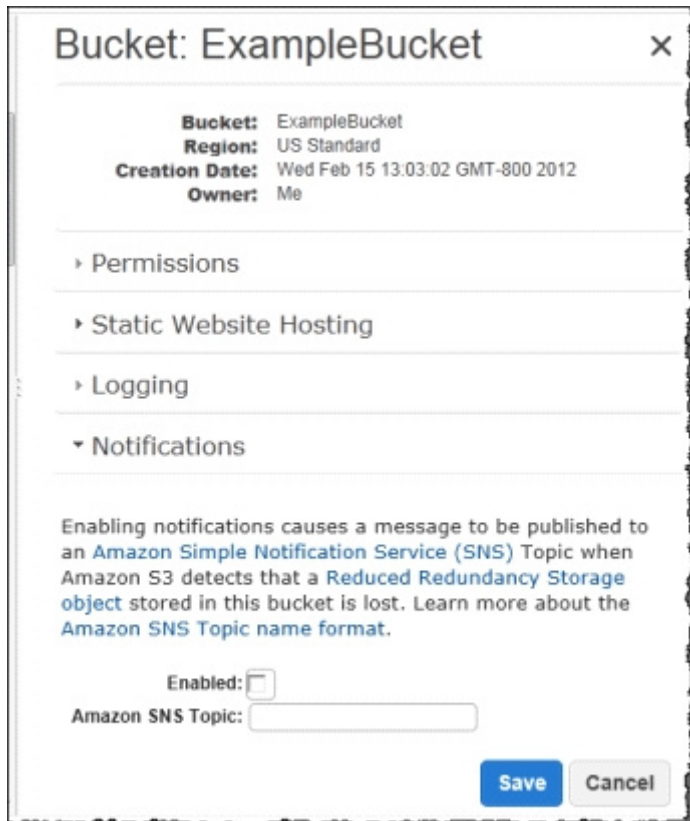
object per year (0.01% of 10,000 objects).

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.



The screenshot shows the 'Bucket: ExampleBucket' configuration page in the Amazon S3 console. The page has a title bar with a close button (X). Below the title, there is a summary section with the following details: Bucket: ExampleBucket, Region: US Standard, Creation Date: Wed Feb 15 13:03:02 GMT-800 2012, and Owner: Me. Below this, there are four expandable sections: Permissions, Static Website Hosting, Logging, and Notifications. The Notifications section is currently expanded, showing a description: '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.' Below the description, there is an 'Enabled:' checkbox which is currently unchecked, and an 'Amazon SNS Topic:' text input field. At the bottom right of the Notifications section, there are 'Save' and 'Cancel' buttons.

QUESTION 26

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 files 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 27

An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 Instances. The customer's security policy requires that every outbound connection from these instances to any other

service within the customer's Virtual Private Cloud must be authenticated using a unique x 509 certificate that contains the specific instance-id.

In addition, an x 509 certificate must be designed by the 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 S3 upon first boot.
- B. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group. Have the launched instances generate a certificate signature request with the instance's assigned instance-id to the key management service for 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 newly launched 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 (that contains the specific instance-id).

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

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 in each 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 each AZ 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 in each AZ inside an Auto Scaling Group behind an ELB 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 in each AZ inside an Auto Scaling Group behind an ELB and a Multi-AZ RDS (Relational Database Service) 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 29

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 30

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 region
- E. 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 31

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 two.)

- 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 32

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

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

- A. Create an EBS backed private AMI which includes a fresh install of your application. Develop a CloudFormation template which includes your AMI and the required EC2, AutoScaling, and ELB resources to support deploying the application across Multiple- Availability-Zones. Asynchronously replicate 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 VPN connection.
- C. Create an EBS backed private AMI which includes a fresh install of your application. Setup a script in your data center to backup the local database every 1 hour and to encrypt and copy the resulting file to an S3 bucket using multi-part upload.
- D. Install your application on a compute-optimized EC2 instance capable of supporting the application's average load. Synchronously replicate transactions from your on-premises database to a database instance in AWS across a secure Direct 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 33

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 the SaaS provider.
- C. Create an IAM role for cross-account access allows the SaaS provider's account to assume the role and assign it a policy that allows only the actions required by the SaaS application.
- D. Create an IAM role for EC2 instances, assign it a policy that allows only the actions required for the SaaS application to work, provide the role ARN to the SaaS provider to use when launching their application instances.

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 cross-account 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

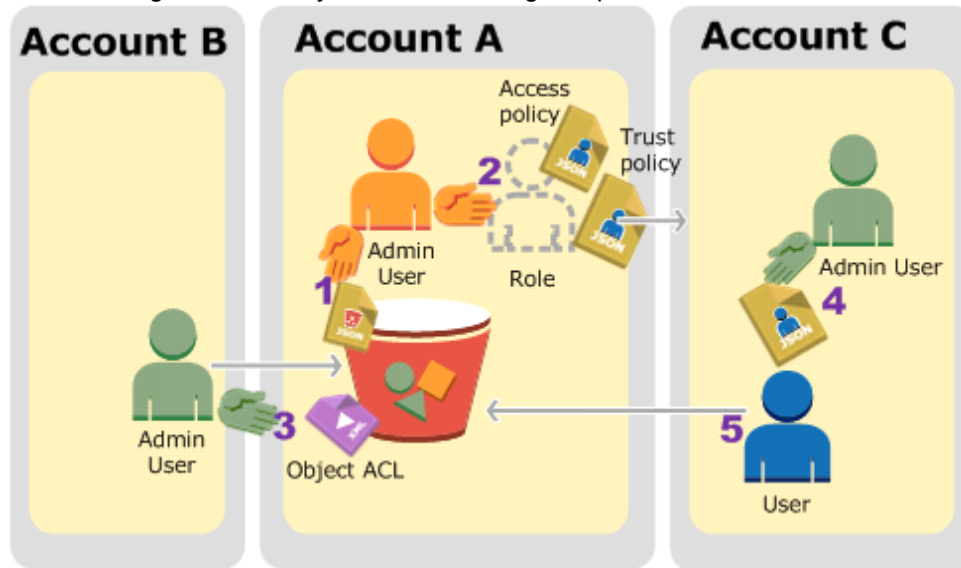
can then do the following to access objects:

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 34

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 35

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 36

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 DynamoDB 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](#).

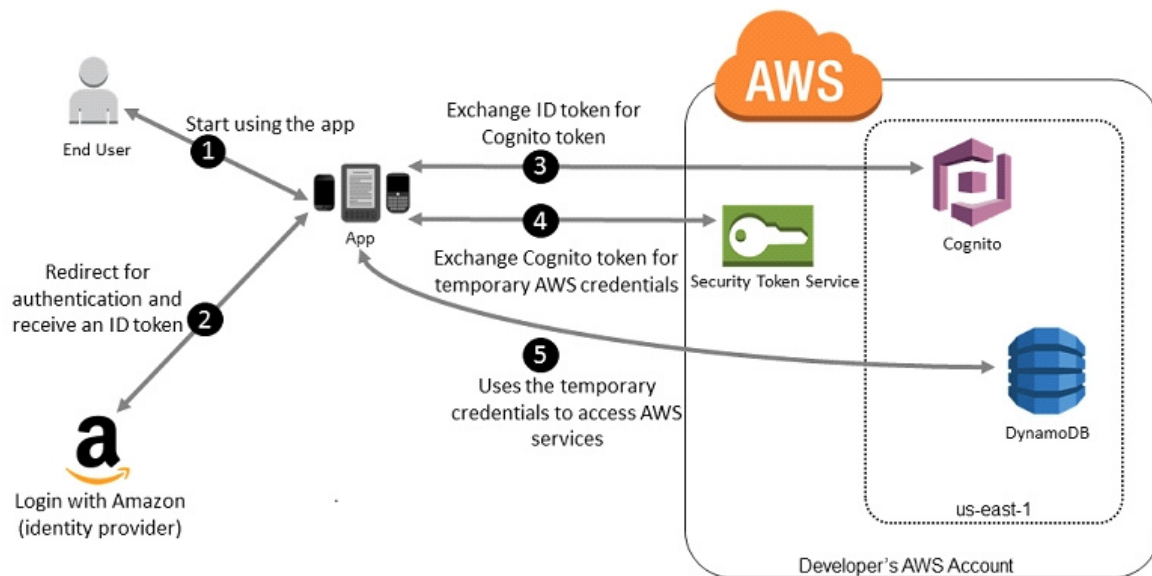
If you don't use Amazon Cognito, then you must write code that interacts with a web IdP (Login with Amazon, Facebook, Google, or any other OIDC-compatible IdP) and then calls the `AssumeRoleWithWebIdentity` API to trade the authentication token you get from those IdPs for AWS temporary security credentials. 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



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 37

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 two.)

- 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 38

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 two.)

- 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)

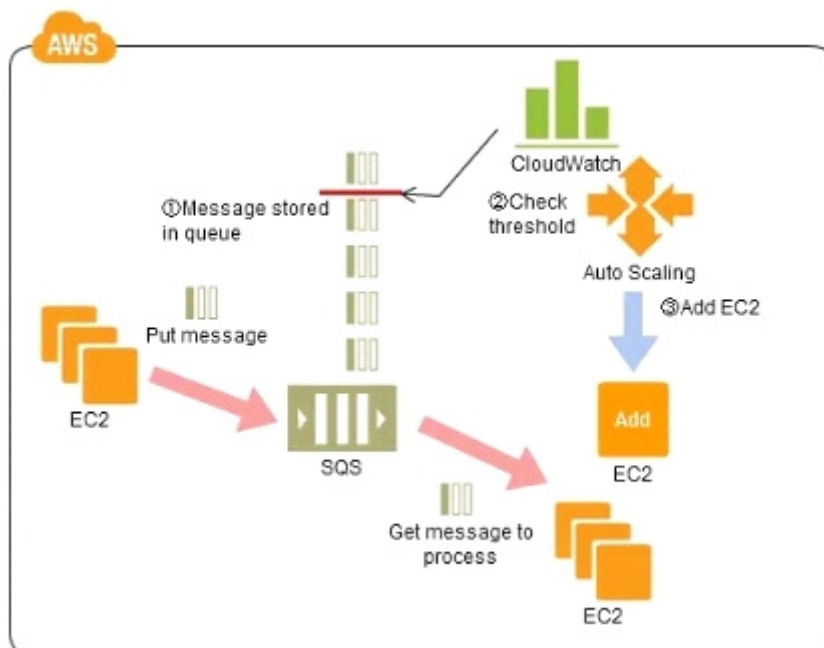
Explanation

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 39



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 time 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 work 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.

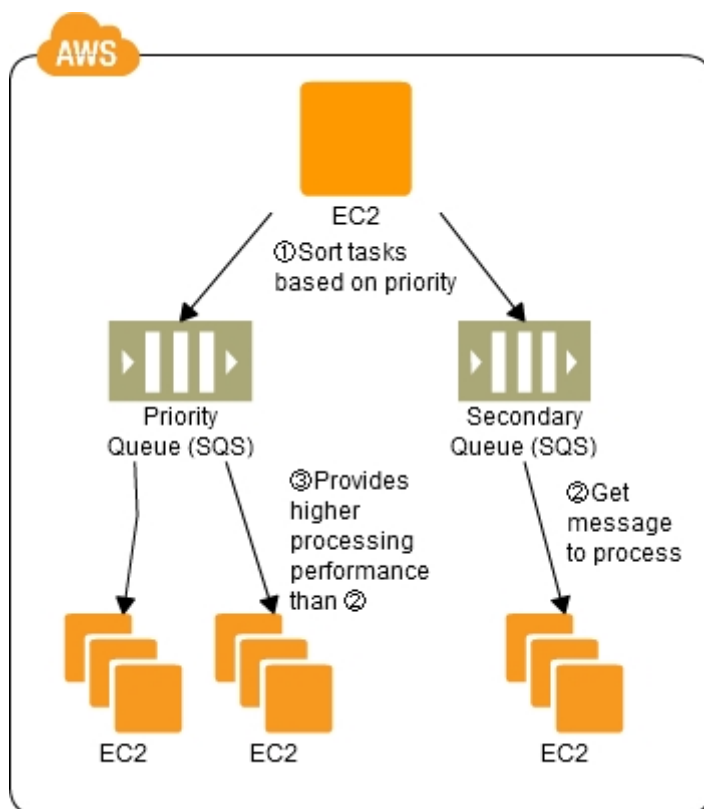
Use SQS to prepare multiple queues for the individual priority levels.

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 40

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 the 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 41

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 three.)

- 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 42

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 three.)

- 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 43

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 two.)

- A. Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials 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 temporary credentials 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 to the appropriate S3 bucket.
- D. The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket.
- 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.

Reference:

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

QUESTION 44

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 will 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 verify network traffic is leveraging DirectConnect.
- B. Configure your DirectConnect router with a higher BGP priority than 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.

Reference:

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

QUESTION 45

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:

Reference:

<http://www.slideshare.net/AmazonWebServices/aws-webcast-introduction-to-amazon-kinesis>

QUESTION 46

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:

Reference:

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

QUESTION 47

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. Manage encryption keys in a Hardware Security Module (HSM) appliance on-premises server 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 store each 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 48

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

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 four.)

- 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 50

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 two.)

- 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 not become healthy, associate the previous launch configuration.
- E. Increase the Elastic Load Balancing Unhealthy Threshold to a higher value to prevent an unhealthy instance from going into service behind the load balancer.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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 52

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

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

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

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

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 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 54

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:

Explanation:

Organizations usually implement proxy solutions to provide URL and web content filtering, IDS/IPS, data loss prevention, monitoring, and advanced threat protection.

Reference: https://d0.awsstatic.com/aws-answers/Controlling_VPC_Egress_Traffic.pdf

QUESTION 55

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 IAM 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:

Reference:

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

QUESTION 56

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": "*"
  }],
  "Condition": {
    "StringEquals": {
      "aws:username": "iam-user-name"
    }
  }
}
```

```

    "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 57

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 58

Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design for the application that leverages multiple regions for the most recently accessed content and latency sensitive portions of the web 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 user preferences 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 each region 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 DynamoDB table 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 ElasticCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of user preferences from a centralized OB to each ElasticCache cluster.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_mediasharing_09.pdf
http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_adserving_06.pdf

QUESTION 59

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 60

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 sessions 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 instances under it. Each EC2 instance implements all 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.

Reference:

<http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html>

QUESTION 61

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-compliant 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 62

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

A benefits enrollment company is hosting a 3-tier web application running in a VPC on AWS which includes a NAT (Network Address Translation) instance in the public Web tier. There is enough provisioned capacity for the expected workload for the new fiscal year benefit enrollment period plus some extra overhead. Enrollment proceeds nicely for two days and then the web tier becomes unresponsive, upon investigation using CloudWatch and other monitoring tools it is discovered that there is an extremely large and unanticipated amount of inbound traffic coming from a set of 15 specific IP addresses over port 80 from a

country where the benefits company has no customers. The web tier instances are so overloaded that benefit 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 64

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Here are some of the things that you can build using fine-grained access control:

A mobile app that displays information for nearby airports, based on the user's location. The app can access and display attributes such as airline names, arrival times, and flight numbers. However, it cannot access or display pilot names or passenger counts.

A mobile game which stores high scores for all users in a single table. Each user can update their own scores, but has no access to the other ones.

Reference:

<https://aws.amazon.com/blogs/aws/fine-grained-access-control-for-amazon-dynamodb/>

QUESTION 65

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 and is therefore only done once per week.

Recently, a new chat feature has been implemented in nodejs and waits 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 66

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:

Explanation:

A default security group is named default, and it has an ID assigned by AWS. The following are the initial settings for each default security group:

Allow inbound traffic only from other instances associated with the default security group Allow all outbound traffic from the instance

The default security group specifies itself as a source security group in its inbound rules. This is what allows instances associated with the default security group to communicate with other instances associated with the default security group.

Reference:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html#default-%20security-group>

QUESTION 67

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:

Reference:

http://docs.aws.amazon.com/workspaces/latest/adminguide/gsg_create_vpc.html

QUESTION 68

Which of the following are characteristics of Amazon VPC subnets? (Choose two.)

- 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: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

In AWS, which security aspects are the customer's responsibility? (Choose four.)

- 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:

Reference:

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

QUESTION 70

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 71

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.

Reference:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions>

QUESTION 72

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 73

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:

Reference:

<https://blog.pythian.com/a-most-simple-cloud-is-amazon-rds-for-oracle-right-for-you/>

QUESTION 74

A 3-tier 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.

Reference:

<https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf>

QUESTION 75

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.

Reference:

<http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html>

QUESTION 76

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:

Reference:

<https://aws.amazon.com/dynamodb/faqs/>

QUESTION 77

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:

Reference:

<https://aws.amazon.com/oracle/>

QUESTION 78

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:

Reference:

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html>

QUESTION 79

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:

Reference:

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

QUESTION 80

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:

Reference:

<http://aws.amazon.com/cognito/faqs/>

QUESTION 81

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.

Reference:

<http://aws.amazon.com/codedeploy/faqs/>

QUESTION 82

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 83

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 84

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 85

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 86

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 87

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 88

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 89

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. 2
- C. 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 90

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 91

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 92

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 colon-delimited 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 93

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 94

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 95

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 96

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 97

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 98

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 99

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 100

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 101

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:InvokeAsync
- D. 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 102

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 103

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. 2
- C. 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 104

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 105

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 106

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 107

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 108

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 109

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 110

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 111

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 112

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 (Amazon 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 113

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 114

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 115

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 116

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 117

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 118

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 119

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 120

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 121

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 122

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 123

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 124

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 125

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 Rights
- D. 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 126

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 127

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 128

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 129

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 130

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 131

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 AWS 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 132

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 133

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 134

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 135

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 136

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 137

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 138

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 139

When using string conditions within IAM, short versions of the available comparators can be used instead of the more verbose ones.

streql 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, streql 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 140

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 141

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 142

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 143

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 144

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 145

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 146

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 147

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 148

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 149

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 150

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 151

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 152

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 153

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 154

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 155

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. `numeqql`

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 156

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 157

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 158

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 159

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 160

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 161

What is a possible reason you would need to edit claims issued in a SAML token?

- A. The NamelIdentifier claim cannot be the same as the username stored in AD.
- B. Authentication fails consistently.
- C. The NamelIdentifier claim cannot be the same as the claim URI.
- D. The NamelIdentifier 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 NamelIdentifier 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 162

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 163

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 164

Do you need to use Amazon Cognito to use the Amazon Mobile Analytics service?

- A. No. However, it is recommended 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 recommends using Amazon Cognito for security best practices.

<http://aws.amazon.com/mobileanalytics/faqs/>

QUESTION 165

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 166

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 167

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 168

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 169

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 170

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 171

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 172

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, 1000BASE-LX (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 173

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 174

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 175

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 176

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 177

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 178

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 179

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 minutes
- C. 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 180

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 181

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 182

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 183

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 AWS's 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 184

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 temporarily

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 185

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 186

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 187

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 188

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 instance
- D. 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 189

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 190

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 191

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 192

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 193

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 194

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 195

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 196

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 197

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:

awscli cloudformation 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 198

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 199

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 200

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 201

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 202

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 203

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 204

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 205

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 206

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 207

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 208

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 center. The user's data center 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 209

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 210

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 211

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 212

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 213

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 subnet
- D. 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 214

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 215

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 two.)

- 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 216

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 217

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 218

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 219

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 220

_____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 221

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 222

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 223

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 224

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 225

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 226

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 227

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 228

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 229

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 230

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 231

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 232

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 233

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 group
- D. 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 234

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 235

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 236

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 requests
- D. 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 237

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 238

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 239

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 240

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 241

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 242

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 243

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: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 244

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: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 245

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 246

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 and allow traffic from the local VPC 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 each service to allow the CIDR ranges of the VPCs in 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 within the 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 and associate 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 of 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 247

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 in the 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: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 248

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 249

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 for the 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 for the 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 250

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 251

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 252

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: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 253

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: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 254

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 Connect connection. 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 data distribution 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 EC2 instances. 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 the Direct Connect connection. Migrate the data distribution website to EC2 instances. By using web servers 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 255

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 the processing completes.
- B. Update the ingestion process to use Amazon Kinesis Data Firehose 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 256

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 jobs 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 257

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 258

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 259

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 solution is 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-region replication 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 Amazon S3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard - 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 old snapshots 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 an hourly AWS Lambda task to copy snapshots from US-EAST -1 to US-WEST-2.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 260

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 templated 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 region, which triggers an AWS Lambda function to populate the cluster in the secondary region.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 261

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 and inform 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 manual information 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 inform Information 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 inform Information Security that this occurred and then shut down the instance.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 262

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 only in 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 AWS Service 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 263

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 for 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 the disaster 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 264

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 NAS server.
- 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 serve the content.
- C. Expose an Amazon EFS share to on-premises users to serve as the NAS server. 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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 265

A company is running a .NET three-tier web application on AWS. The team currently uses XL storage optimized instances to store and 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. Enable Amazon 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 instances to 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.xl instances needed to meet base performance requirements.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 266

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 Amazon Rekognition. 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 Amazon Rekognition. 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. Configure Amazon 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 on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required 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 267

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 268

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 shared services 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 resource record 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 with resource 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 269

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 270

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: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 271

A company with 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 1111-1111-1111:

```
{
  "Version": "2012-10-17",
  "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 272

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 273

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 group
- D. Replace the application tier with 4 m4.2xlarge instances

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 274

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 scheduled 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 new Amazon 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 instances behind 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 ES cluster. 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 275

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 than the 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 on the database to trigger a DNS failover to the standby region if the health checks in the primary region 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 53 health 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 276

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 is a cost effective way to 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 277

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. Use Amazon 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 states directly 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 and visualized 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 AWS Lambda processing logs to see the workflow states.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 278

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 the inventory 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 279

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 assume and 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 on the 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 data from 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 the bucket. Have the organizations assume and use that read role when accessing the data.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 280

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 Connect fails.
- 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 VPN connection.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 281

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: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 282

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 using AWS 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 newest version, 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 283

The company Security team requires 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 CloudHSM client software to control access to the keys that 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 in CloudHSM.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 284

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 WorkSpaces Workspace 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 Amazon AppStream 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 to improve 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 Amazon CloudFront to improve the user experience.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 285

A company needs to run a software package that has a license that must be run on the same physical host for the duration of its use. The software package is only going to be used for 90 days. The company requires patching and restarting of all instances every 30 days.

How can these requirements be met using AWS?

- A. Run a dedicated instance with auto-placement disabled.
- B. Run the instance on a dedicated host with Host Affinity set to `Host`.
- C. Run an On-Demand Instance with a Reserved Instance to ensure consistent placement.
- D. Run the instance on a licensed host with termination set for 90 days.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 286

A bank is designing an online customer service portal where customers can chat with customer service agents. The portal is required to maintain a 15-minute RPO or RTO in case of a regional disaster. Banking regulations require that all customer service chat transcripts must be preserved on durable storage for at least 7 years, chat conversations must be encrypted in-flight, and transcripts must be encrypted at rest. The Data Loss Prevention team requires that data at rest must be encrypted using a key that the team controls, rotates, and revokes.

Which design meets these requirements?

- A. The chat application logs each chat message into Amazon CloudWatch Logs. A scheduled AWS Lambda function invokes a CloudWatch Logs `CreateExportTask` every 5 minutes to export chat transcripts to Amazon S3. The S3 bucket is configured for cross-region replication to the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the S3 bucket.
- B. The chat application logs each chat message into two different Amazon CloudWatch Logs groups in two different regions, with the same AWS KMS key applied. Both CloudWatch Logs groups are configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy with a KMS key specified.
- C. The chat application logs each chat message into Amazon CloudWatch Logs. A subscription filter on the CloudWatch Logs group feeds into an Amazon Kinesis Data Firehose which streams the chat messages into an Amazon S3 bucket in the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Kinesis Data Firehose.
- D. The chat application logs each chat message into Amazon CloudWatch Logs. The CloudWatch Logs group is configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy. Glacier cross-region replication mirrors chat archives to the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Amazon Glacier vault.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 287

A company currently runs a secure application on Amazon EC2 that takes files from on-premises locations through AWS Direct Connect, processes them, and uploads them to a single Amazon S3 bucket. The application uses HTTPS for encryption in transit to Amazon S3, and S3 server-side encryption to encrypt at rest.

Which of the following changes should the Solutions Architect recommend to make this solution more secure without impeding application's performance?

- A. Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the NAT gateway's Elastic IP address only.
- B. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required Amazon S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC's source IP range only.

- C. Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the source public IP address of the on-premises network only.
- D. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC endpoint only.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 288

A company has more than 100 AWS accounts, with one VPC per account, that need outbound HTTPS connectivity to the internet. The current design contains one NAT gateway per Availability Zone (AZ) in each VPC. To reduce costs and obtain information about outbound traffic, management has asked for a new architecture for internet access.

Which solution will meet the current needs, and continue to grow as new accounts are provisioned, while reducing costs?

- A. Create a transit VPC across two AZs using a third-party routing appliance. Create a VPN connection to each VPC. Default route internet traffic to the transit VPC.
- B. Create multiple hosted-private AWS Direct Connect VIFs, one per account, each with a Direct Connect gateway. Default route internet traffic back to an on-premises router to route to the internet.
- C. Create a central VPC for outbound internet traffic. Use VPC peering to default route to a set of redundant NAT gateway in the central VPC.
- D. Create a proxy fleet in a central VPC account. Create an AWS PrivateLink endpoint service in the central VPC. Use PrivateLink interface for internet connectivity through the proxy fleet.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 289

A company is migrating its marketing website and content management system from an on-premises data center to AWS. The company wants the AWS application to be deployed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database.

The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers. After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.

How can the application and environment be deployed and automated in AWS, while allowing for future changes?

- A. Update the runbook to describe how to create the VPC, the EC2 instances, and the RDS instance for the application by using the AWS Console. Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.
- B. Write a Python script that uses the AWS API to create the VPC, the EC2 instances, and the RDS instance for the application. Write shell scripts that implement the rest of the steps in the runbook. Have the Python script copy and run the shell scripts on the newly created instances to complete the installation.
- C. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS

instance for the application. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.

- D. Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Include EC2 user data in the AWS CloudFormation template to install and configure the software.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 290

A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4. Company policy requires systems that communicate with external vendors to use a security group that limits access to only approved external vendors. The virtual private cloud (VPC) uses the default network ACL.

The Systems Operator successfully assigns IPv6 addresses to each of the backend systems. The Systems Operator also updates the outbound security group to include the IPv6 CIDR of the external vendor (destination). The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor.

What changes are required to enable communication with the external vendor?

- A. Create an IPv6 NAT instance. Add a route for destination 0.0.0.0/0 pointing to the NAT instance.
- B. Enable IPv6 on the NAT gateway. Add a route for destination ::/0 pointing to the NAT gateway.
- C. Enable IPv6 on the internet gateway. Add a route for destination 0.0.0.0/0 pointing to the IGW.
- D. Create an egress-only internet gateway. Add a route for destination ::/0 pointing to the gateway.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 291

A Solutions Architect is designing the storage layer for a data warehousing application. The data files are large, but they have statically placed metadata at the beginning of each file that describes the size and placement of the file's index. The data files are read in by a fleet of Amazon EC2 instances that store the index size, index location, and other category information about the data file in a database. That database is used by Amazon EMR to group files together for deeper analysis.

What would be the MOST cost-effective, high availability storage solution for this workflow?

- A. Store the data files in Amazon S3 and use Range GET for each file's metadata, then index the relevant data.
- B. Store the data files in Amazon EFS mounted by the EC2 fleet and EMR nodes.
- C. Store the data files on Amazon EBS volumes and allow the EC2 fleet and EMR to mount and unmount the volumes where they are needed.
- D. Store the content of the data files in Amazon DynamoDB tables with the metadata, index, and data as their own keys.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 292

A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory, and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications.

Which solution meets the requirements by using the LEAST amount of management overhead?

- A. Connect the Active Directory to AWS by using single sign-on and an Active Directory Federation Services (AD FS) with SAML 2.0, and then configure the Identity Provider (IdP) system to use form-based authentication. Build the AD FS portal page with corporate branding, and integrate third-party applications that support SAML 2.0 as required.
- B. Create a two-way Forest trust relationship between the on-premises Active Directory and the AWS Directory Service. Set up AWS Single Sign-On with AWS Organizations. Use single sign-on integrations for connections with third-party applications.
- C. Configure single sign-on by connecting the on-premises Active Directory using the AWS Directory Service AD Connector. Enable federation to the AWS services and accounts by using the IAM applications and services linking function. Leverage third-party single sign-on as needed.
- D. Connect the company's Active Directory to AWS by using AD FS and SAML 2.0. Configure the AD FS claim rule to leverage Regex and a common Active Directory naming convention for the security group to allow federation of all AWS accounts. Leverage third-party single sign-on as needed, and add it to the AD FS server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 293

A Solutions Architect is designing a network solution for a company that has applications running in a data center in Northern Virginia. The applications in the company's data center require predictable performance to applications running in a virtual private cloud (VPC) located in us-east-1, and a secondary VPC in us-west-2 within the same account. The company data center is collocated in an AWS Direct Connect facility that serves the us-east-1 region. The company has already ordered an AWS Direct Connect connection and a cross-connect has been established.

Which solution will meet the requirements at the LOWEST cost?

- A. Provision a Direct Connect gateway and attach the virtual private gateway (VGW) for the VPC in us-east-1 and the VGW for the VPC in us-west-2. Create a private VIF on the Direct Connect connection and associate it to the Direct Connect gateway.
- B. Create private VIFs on the Direct Connect connection for each of the company's VPCs in the us-east-1 and us-west-2 regions. Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFs.
- C. Deploy a transit VPC solution using Amazon EC2-based router instances in the us-east-1 region. Establish IPsec VPN tunnels between the transit routers and virtual private gateways (VGWs) located in the us-east-1 and us-west-2 regions, which are attached to the company's VPCs in those regions. Create a public VIF on the Direct Connect connection and establish IPsec VPN tunnels over the public VIF between the transit routers and the company's data center router.
- D. Order a second Direct Connect connection to a Direct Connect facility with connectivity to the us-west-2 region. Work with a partner to establish a network extension link over dark fiber from the Direct Connect facility to the company's data center. Establish private VIFs on the Direct Connect connections for each of the company's VPCs in the respective regions. Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFs.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 294

A company operating a website on AWS requires high levels of scalability, availability, and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage. Amazon CloudFront is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution.

Which solution is the MOST cost-effective at scale?

- A. Implement Multi-AZ and Auto Scaling for all EC2 instances in the current configuration. Ensure that all EC2 instances are purchased as reserved instances. Implement new elastic Amazon EBS volumes for the data tier.
- B. Design and implement the Docker-based containerized solution for the application using Amazon ECS. Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow the Aurora MySQL storage, as necessary. Ensure that Multi-AZ architectures are implemented.
- C. Ensure that EC2 instances are right-sized and behind an Elastic Load Balancing load balancer. Implement Auto Scaling with EC2 instances. Ensure that the reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand. Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Ensure that Multi-AZ architectures are implemented.
- D. Ensure that EC2 instances are right-sized and behind an Elastic Load Balancer. Implement Auto Scaling with EC2 instances. Ensure that Reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand. Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow Aurora MySQL storage, as necessary. Ensure Multi-AZ architectures are implemented.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 295

The Security team needs to provide a team of interns with an AWS environment so they can build a serverless video transcoding application. The project will use Amazon S3, AWS Lambda, Amazon API Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder.

The interns should be able to create and configure the necessary resources, but they may not have access to create or modify AWS IAM roles. The Solutions Architect creates a policy and attaches it to the interns' group.

How should the Security team configure the environment to ensure that the interns are self-sufficient?

- A. Create a policy that allows creation of project-related resources only. Create roles with required service permissions, which are assumable by the services.
- B. Create a policy that allows creation of all project-related resources, including roles that allow access only to specified resources.
- C. Create roles with the required service permissions, which are assumable by the services. Have the interns create and use a bastion host to create the project resources in the project subnet only.
- D. Create a policy that allows creation of project-related resources only. Require the interns to raise a request for roles to be created with the Security team. The interns will provide the requirements for the permissions to be set in the role.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 296

A large multinational company runs a timesheet application on AWS that is used by staff across the world. The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer, and stores data in an Amazon RDS MySQL Multi-AZ database instance.

The CFO is concerned about the impact on the business if the application is not available. The application must not be down for more than two hours, but the solution must be as cost-effective as possible.

How should the Solutions Architect meet the CFO's requirements while minimizing data loss?

- A. In another region, configure a read replica and create a copy of the infrastructure. When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance. Update the DNS record to point to the other region's ELB.
- B. Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance. Create an AWS CloudFormation template of the application infrastructure that uses the latest snapshot. When an issue occurs, use the AWS CloudFormation template to create the environment in another region. Update the DNS record to point to the other region's ELB.
- C. Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance which is copied to another region. Create an AWS CloudFormation template of the application infrastructure that uses the latest copied snapshot. When an issue occurs, use the AWS CloudFormation template to create the environment in another region. Update the DNS record to point to the other region's ELB.
- D. Configure a read replica in another region. Create an AWS CloudFormation template of the application infrastructure. When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance and use the AWS CloudFormation template to create the environment in another region using the promoted Amazon RDS instance. Update the DNS record to point to the other region's ELB.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 297

A Development team has created a series of AWS CloudFormation templates to help deploy services. They created a template for a network/virtual private cloud (VPC) stack, a database stack, a bastion host stack, and a web application-specific stack. Each service requires the deployment of at least:

- A network/VPC stack
- A bastion host stack
- A web application stack

Each template has multiple input parameters that make it difficult to deploy the services individually from the AWS CloudFormation console. The input parameters from one stack are typically outputs from other stacks. For example, the VPC ID, subnet IDs, and security groups from the network stack may need to be used in the application stack or database stack.

Which actions will help reduce both the operational burden and the number of parameters passed into a service deployment? (Choose two.)

- A. Create a new AWS CloudFormation template for each service. Alter the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Call the newly created service stack from the AWS CloudFormation console to deploy the specific service with a subset of the parameters previously required.
- B. Create a new portfolio in AWS Service Catalog for each service. Create a product for each existing

AWS CloudFormation template required to build the service. Add the products to the portfolio that represents that service in AWS Service Catalog. To deploy the service, select the specific service portfolio and launch the portfolio with the necessary parameters to deploy all templates.

- C. Set up an AWS CodePipeline workflow for each service. For each existing template, choose AWS CloudFormation as a deployment action. Add the AWS CloudFormation template to the deployment action. Ensure that the deployment actions are processed to make sure that dependencies are obeyed. Use configuration files and scripts to share parameters between the stacks. To launch the service, execute the specific template by choosing the name of the service and releasing a change.
- D. Use AWS Step Functions to define a new service. Create a new AWS CloudFormation template for each service. Alter the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new service template. Configure AWS Step Functions to call the service template directly. In the AWS Step Functions console, execute the step.
- E. Create a new portfolio for the services in AWS Service Catalog. Create a new AWS CloudFormation template for each service. Alter the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Create a product for each application. Add the service template to the product. Add each new product to the portfolio. Deploy the product from the portfolio to deploy the service with the necessary parameters only to start the deployment.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 298

A company wants to replace its call center system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the callers and handle basic tasks, reducing the need to speak to an agent. The solution should also be able to query business applications and provide relevant information back to callers as requested.

Which services should the Solutions Architect use to build this solution? (Choose three.)

- A. Amazon Rekognition to identify who is calling.
- B. Amazon Connect to create a cloud-based contact center.
- C. Amazon Alexa for Business to build conversational interfaces.
- D. AWS Lambda to integrate with internal systems.
- E. Amazon Lex to recognize the intent of the caller.
- F. Amazon SQS to add incoming callers to a queue.

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 299

An internal security audit of AWS resources within a company found that a number of Amazon EC2 instances running Microsoft Windows workloads were missing several important operating system-level patches. A Solutions Architect has been asked to fix existing patch deficiencies, and to develop a workflow to ensure that future patching requirements are identified and taken care of quickly. The Solutions Architect has decided to use AWS Systems Manager. It is important that EC2 instance reboots do not occur at the same time on all Windows workloads to meet organizational uptime requirements.

Which workflow will meet these requirements in an automated manner?

- A. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline to the Windows Servers patch group. Define an AWS Systems Manager maintenance window, conduct patching within it, and associate it with the Windows Servers patch group. Register instances with the maintenance window using associated subnet IDs. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.
- B. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline to the Windows Servers patch group. Create an Amazon CloudWatch Events rule configured to use a cron expression to schedule the execution of patching using the AWS Systems Manager `run` command. Assign the AWS-RunWindowsPatchBaseline document as a task associated with the Windows Servers patch group. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.
- C. Add a Patch Group tag with a value of either Windows Servers1 or Windows Servers2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Register targets with specific maintenance windows using the Patch Group tags. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.
- D. Add a Patch Group tag with a value of either Windows Servers1 or Windows Server2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Assign the AWS-RunWindowsPatchBaseline document as a task within each maintenance window. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 300

A company deployed a three-tier web application in two regions: us-east-1 and eu-west-1. The application must be active in both regions at the same time. The database tier of the application uses a single Amazon RDS Aurora database globally, with a master in us-east-1 and a read replica in eu-west-1. Both regions are connected by a VPN.

The company wants to ensure that the application remains available even in the event of a region-level failure of all of the application's components. It is acceptable for the application to be in read-only mode for up to 1 hour. The company plans to configure two Amazon Route 53 record sets, one for each of the regions.

How should the company complete the configuration to meet its requirements while providing the lowest latency for the application end-users? (Choose two.)

- A. Use failover routing and configure the us-east-1 record set as primary and the eu-west-1 record set as secondary. Configure an HTTP health check for the web application in us-east-1, and associate it to the us-east-1 record set.
- B. Use weighted routing and configure each record set with a weight of 50. Configure an HTTP health check for each region, and attach it to the record set for that region.
- C. Use latency-based routing for both record sets. Configure a health check for each region and attach it to the record set for that region.
- D. Configure an Amazon CloudWatch alarm for the health checks in us-east-1, and have it invoke an AWS Lambda function that promotes the read replica in eu-west-1.
- E. Configure Amazon RDS event notifications to react to the failure of the database in us-east-1 by invoking an AWS Lambda function that promotes the read replica in eu-west-1.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 301

A company runs a Windows Server host in a public subnet that is configured to allow a team of administrators to connect over RDP to troubleshoot issues with hosts in a private subnet. The host must be available at all times outside of a scheduled maintenance window, and needs to receive the latest operating system updates within 3 days of release.

What should be done to manage the host with the LEAST amount of administrative effort?

- A. Run the host in a single-instance AWS Elastic Beanstalk environment. Configure the environment with a custom AMI to use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch Manager.
- B. Run the host on AWS WorkSpaces. Use Amazon WorkSpaces Application Manager (WAM) to harden the host. Configure Windows automatic updates to occur every 3 days.
- C. Run the host in an Auto Scaling group with a minimum and maximum instance count of 1. Use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch Manager.
- D. Run the host in AWS OpsWorks Stacks. Use a Chef recipe to harden the AMI during instance launch. Use an AWS Lambda scheduled event to run the Upgrade Operating System stack command to apply system updates.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 302

A company has a large on-premises Apache Hadoop cluster with a 20 PB HDFS database. The cluster is growing every quarter by roughly 200 instances and 1 PB. The company's goals are to enable resiliency for its Hadoop data, limit the impact of losing cluster nodes, and significantly reduce costs. The current cluster runs 24/7 and supports a variety of analysis workloads, including interactive queries and batch processing.

Which solution would meet these requirements with the LEAST expense and down time?

- A. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster. Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized.
- B. Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster of a similar size and configuration to the current cluster. Store the data on EMRFS. Minimize costs by using Reserved Instances. As the workload grows each quarter, purchase additional Reserved Instances and add to the cluster.
- C. Use AWS Snowball to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workloads based on historical data from the on-premises cluster. Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized.
- D. Use AWS Direct Connect to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster. Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 303

A company has a requirement that only allows specially hardened AMIs to be launched into public subnets in a VPC, and for the AMIs to be associated with a specific security group. Allowing non-compliant instances to launch into the public subnet could present a significant security risk if they are allowed to operate.

A mapping of approved AMIs to subnets to security groups exists in an Amazon DynamoDB table in the same AWS account. The company created an AWS Lambda function that, when invoked, will terminate a given Amazon EC2 instance if the combination of AMI, subnet, and security group are not approved in the DynamoDB table.

What should the Solutions Architect do to MOST quickly mitigate the risk of compliance deviations?

- A. Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched using one of the allowed AMIs, and associate it with the Lambda function as the target.
- B. For the Amazon S3 bucket receiving the AWS CloudTrail logs, create an S3 event notification configuration with a filter to match when logs contain the `ec2:RunInstances` action, and associate it with the Lambda function as the target.
- C. Enable AWS CloudTrail and configure it to stream to an Amazon CloudWatch Logs group. Create a metric filter in CloudWatch to match when the `ec2:RunInstances` action occurs, and trigger the Lambda function when the metric is greater than 0.
- D. Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched, and associate it with the Lambda function as the target.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 304

A Solutions Architect must migrate an existing on-premises web application with 70 TB of static files supporting a public open-data initiative. The Architect wants to upgrade to the latest version of the host operating system as part of the migration effort.

Which is the FASTEST and MOST cost-effective way to perform the migration?

- A. Run a physical-to-virtual conversion on the application server. Transfer the server image over the internet, and transfer the static data to Amazon S3.
- B. Run a physical-to-virtual conversion on the application server. Transfer the server image over AWS Direct Connect, and transfer the static data to Amazon S3.
- C. Re-platform the server to Amazon EC2, and use AWS Snowball to transfer the static data to Amazon S3.
- D. Re-platform the server by using the AWS Server Migration Service to move the code and data to a new Amazon EC2 instance.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 305

A company has an application that generates a weather forecast that is updated every 15 minutes with an output resolution of 1 billion unique positions, each approximately 20 bytes in size (20 Gigabytes per forecast). Every hour, the forecast data is globally accessed approximately 5 million times (1,400 requests per second), and up to 10 times more during weather events. The forecast data is overwritten every update. Users of the current weather forecast application expect responses to queries to be returned in less than two seconds for each request.

Which design meets the required request rate and response time?

- A. Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Enable API caching on the API Gateway stage with a cache-control timeout set for 15 minutes.
- B. Store forecast locations in an Amazon EFS volume. Create an Amazon CloudFront distribution that targets an Elastic Load Balancing group of an Auto Scaling fleet of Amazon EC2 instances that have mounted the Amazon EFS volume. Set the cache-control timeout for 15 minutes in the CloudFront distribution.
- C. Store forecast locations in an Amazon S3 bucket. Use an Amazon CloudFront distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Create an Amazon Lambda@Edge function that caches the data locally at edge locations for 15 minutes.
- D. Store forecast locations in Amazon S3 as individual objects. Create an Amazon CloudFront distribution targeting an Elastic Load Balancing group of an Auto Scaling fleet of EC2 instances, querying the origin of the S3 object. Set the cache-control timeout for 15 minutes in the CloudFront distribution.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 306

A company is using AWS to run an internet-facing production application written in Node.js. The Development team is responsible for pushing new versions of their software directly to production. The application software is updated multiple times a day. The team needs guidance from a Solutions Architect to help them deploy the software to the production fleet quickly and with the least amount of disruption to the service.

Which option meets these requirements?

- A. Prepackage the software into an AMI and then use Auto Scaling to deploy the production fleet. For software changes, update the AMI and allow Auto Scaling to automatically push the new AMI to production.
- B. Use AWS CodeDeploy to push the prepackaged AMI to production. For software changes, reconfigure CodeDeploy with new AMI identification to push the new AMI to the production fleet.
- C. Use AWS Elastic Beanstalk to host the production application. For software changes, upload the new application version to Elastic Beanstalk to push this to the production fleet using a blue/green deployment method.
- D. Deploy the base AMI through Auto Scaling and bootstrap the software using user data. For software changes, SSH to each of the instances and replace the software with the new version.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 307

A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume.

The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos.

Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?

- A. Reconfigure Amazon EFS to enable maximum I/O.
- B. Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.
- C. Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.
- D. Set up an Amazon CloudFront distribution for all site contents, and point the distribution at the ALB.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 308

A company runs its containerized batch jobs on Amazon ECS. The jobs are scheduled by submitting a container image, a task definition, and the relevant data to an Amazon S3 bucket. Container images may be unique per job. Running the jobs as quickly as possible is of utmost importance, so submitting job artifacts to the S3 bucket triggers the job to run immediately. Sometimes there may be no jobs running at all. However, jobs of any size can be submitted with no prior warning to the IT Operations team. Job definitions include CPU and memory resource requirements.

What solution will allow the batch jobs to complete as quickly as possible after being scheduled?

- A. Schedule the jobs on an Amazon ECS cluster using the Amazon EC2 launch type. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.
- B. Schedule the jobs directly on EC2 instances. Use Reserved Instances for the baseline minimum load, and use On-Demand Instances in an Auto Scaling group to scale up the platform based on demand.
- C. Schedule the jobs on an Amazon ECS cluster using the Fargate launch type. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.
- D. Schedule the jobs on an Amazon ECS cluster using the Fargate launch type. Use Spot Instances in an Auto Scaling group to scale the platform based on demand. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 309

A company receives clickstream data files to Amazon S3 every five minutes. A Python script runs as a cron job once a day on an Amazon EC2 instance to process each file and load it into a database hosted on Amazon RDS. The cron job takes 15 to 30 minutes to process 24 hours of data. The data consumers ask for the data be available as soon as possible.

Which solution would accomplish the desired outcome?

- A. Increase the size of the instance to speed up processing and update the schedule to run once an hour.
- B. Convert the cron job to an AWS Lambda function and trigger this new function using a cron job on an EC2 instance.
- C. Convert the cron job to an AWS Lambda function and schedule it to run once an hour using Amazon CloudWatch Events.

- D. Create an AWS Lambda function that runs when a file is delivered to Amazon S3 using S3 event notifications.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 310

A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume. The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency. Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas
- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
- D. Use AWS-X-Ray to analyze and debug application issues and add more API servers to match the load
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 311

A Solutions Architect is designing a system that will collect and store data from 2,000 internet-connected sensors. Each sensor produces 1 KB of data every second. The data must be available for analysis within a few seconds of it being sent to the system and stored for analysis indefinitely. Which is the MOST cost-effective solution for collecting and storing the data?

- A. Put each record in Amazon Kinesis Data Streams. Use an AWS Lambda function to write each record to an object in Amazon S3 with a prefix that organizes the records by hour and hashes the record's key. Analyze recent data from Kinesis Data Streams and historical data from Amazon S3.
- B. Put each record in Amazon Kinesis Data Streams. Set up Amazon Kinesis Data Firehose to read records from the stream and group them into objects in Amazon S3. Analyze recent data from Kinesis Data Streams and historical data from Amazon S3.
- C. Put each record into an Amazon DynamoDB table. Analyze the recent data by querying the table. Use an AWS Lambda function connected to a DynamoDB stream to group records together, write them into objects in Amazon S3, and then delete the record from the DynamoDB table. Analyze recent data from the DynamoDB table and historical data from Amazon S3
- D. Put each record into an object in Amazon S3 with a prefix what organizes the records by hour and hashes the record's key. Use S3 lifecycle management to transition objects to S3 infrequent access storage to reduce storage costs. Analyze recent and historical data by accessing the data in Amazon S3

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 312

An auction website enables users to bid on collectible items. The auction rules require that each bid is processed only once and in the order it was received. The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis Data Streams. A single t2.large instance has a cron job that runs the bid processor, which reads incoming bids from Kinesis Data Streams and processes each bid. The auction site is growing in popularity, but users are complaining that some bids are not registering.

Troubleshooting indicates that the bid processor is too slow during peak demand hours, sometimes crashes while processing, and occasionally loses track of which records is being processed.

What changes should make the bid processing more reliable?

- A. Refactor the web application to use the Amazon Kinesis Producer Library (KPL) when posting bids to Kinesis Data Streams. Refactor the bid processor to flag each record in Kinesis Data Streams as being unread, processing, and processed. At the start of each bid processing run, scan Kinesis Data Streams for unprocessed records.
- B. Refactor the web application to post each incoming bid to an Amazon SNS topic in place of Kinesis Data Streams. Configure the SNS topic to trigger an AWS Lambda function that processes each bid as soon as a user submits it.
- C. Refactor the web application to post each incoming bid to an Amazon SQS FIFO queue in place of Kinesis Data Streams. Refactor the bid processor to continuously poll the SQS queue. Place the bid processing EC2 instance in an Auto Scaling group with a minimum and a maximum size of 1.
- D. Switch the EC2 instance type from t2.large to a larger general compute instance type. Put the bid processor EC2 instances in an Auto Scaling group that scales out the number of EC2 instances running the bid processor, based on the IncomingRecords metric in Kinesis Data Streams.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 313

A bank is re-architecting its mainframe-based credit card approval processing application to a cloud-native application on the AWS cloud.

The new application will receive up to 1,000 requests per second at peak load. There are multiple steps to each transaction, and each step must receive the result of the previous step. The entire request must return an authorization response within less than 2 seconds with zero data loss. Every request must receive a response. The solution must be Payment Card Industry Data Security Standard (PCI DSS)-compliant.

Which option will meet all of the bank's objectives with the LEAST complexity and LOWEST cost while also meeting compliance requirements?

- A. Create an Amazon API Gateway to process inbound requests using a single AWS Lambda task that performs multiple steps and returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application.
- B. Create an Application Load Balancer with an Amazon ECS cluster on Amazon EC2 Dedicated Instances in a target group to process incoming requests. Use Auto Scaling to scale the cluster out/in based on average CPU utilization. Deploy a web service that processes all of the approval steps and returns a JSON object with the approval status.
- C. Deploy the application on Amazon EC2 on Dedicated Instances. Use an Elastic Load Balancer in front of a farm of application servers in an Auto Scaling group to handle incoming requests. Scale out/in based on a custom Amazon CloudWatch metric for the number of inbound requests per second after measuring the capacity of a single instance.
- D. Create an Amazon API Gateway to process inbound requests using a series of AWS Lambda processes, each with an Amazon SQS input queue. As each step completes, it writes its result to the next step's queue. The final step returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 314

A Solutions Architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The Solutions Architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.

What should be done next to complete the update?

- A. Redirect to the new environment using Amazon Route 53
- B. Select the Swap Environment URLs option
- C. Replace the Auto Scaling launch configuration
- D. Update the DNS records to point to the green environment

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 315

A photo-sharing and publishing company receives 10,000 to 150,000 images daily. The company receives the images from multiple suppliers and users registered with the service. The company is moving to AWS and wants to enrich the existing metadata by adding data using Amazon Rekognition.

The following is an example of the additional data:

```
list celebrities [name of the personality] wearing [color] looking  
[happy, sad] near [location example Eiffel Tower in Paris]
```

As part of the cloud migration program, the company uploaded existing image data to Amazon S3 and told users to upload images directly to Amazon S3.

What should the Solutions Architect do to support these requirements?

- A. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon DynamoDB to store the metadata and Amazon ES to create an index. Use a web front-end to provide search capabilities backed by Amazon ES.
- B. Use Amazon Kinesis to stream data based on an S3 event. Use an application running in Amazon EC2 to extract metadata from the images. Then store the data on Amazon DynamoDB and Amazon CloudSearch and create an index. Use a web front-end with search capabilities backed by CloudSearch.
- C. Start an Amazon SQS queue based on S3 event notifications. Then have Amazon SQS send the metadata information to Amazon DynamoDB. An application running on Amazon EC2 extracts data from Amazon Rekognition using the API and adds data to DynamoDB and Amazon ES. Use a web front-end to provide search capabilities backed by Amazon ES.
- D. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon RDS MySQL Multi-AZ to store the metadata information and use Lambda to create an index. Use a web front-end with search capabilities backed by Lambda.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 316

A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept. Amazon CloudWatch metrics did not indicate any issues with DynamoDB but showed that some Lambda functions were hitting their timeout.

Which of the following actions should the Solutions Architect consider to improve performance? (Choose two.)

- A. Configure the AWS Lambda function to reuse containers to avoid unnecessary startup time.
- B. Increase the amount of memory and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal memory and timeout configuration for the Lambda function.
- C. Create an Amazon ElastiCache cluster running Memcached, and configure the Lambda function for VPC integration with access to the Amazon ElastiCache cluster.
- D. Enable API cache on the appropriate stage in Amazon API Gateway, and override the TTL for individual methods that require a lower TTL than the entire stage.
- E. Increase the amount of CPU, and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal CPU and timeout configuration for the Lambda function.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 317

A Solutions Architect is designing a highly available and reliable solution for a cluster of Amazon EC2 instances.

The Solutions Architect must ensure that any EC2 instance within the cluster recovers automatically after a system failure. The solution must ensure that the recovered instance maintains the same IP address.

How can these requirements be met?

- A. Create an AWS Lambda script to restart any EC2 instances that shut down unexpectedly.
- B. Create an Auto Scaling group for each EC2 instance that has a minimum and maximum size of 1.
- C. Create a new t2.micro instance to monitor the cluster instances. Configure the t2.micro instance to issue an `aws ec2 reboot-instances` command upon failure.
- D. Create an Amazon CloudWatch alarm for the `StatusCheckFailed_System` metric, and then configure an EC2 action to recover the instance.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 318

A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check.

Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times.

Which of the following changes together would remediate these issues while improving monitoring

capabilities for the availability and functionality of the entire application stack for future growth? (Choose two.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
- E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 319

A company is running an email application across multiple AWS Regions. The company uses Ohio (us-east-2) as the primary Region and Northern Virginia (us-east-1) as the Disaster Recovery (DR) Region. The data is continuously replicated from the primary Region to the DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time, but it affects the application's RPO.

Which of the following solutions should help remediate this performance problem? (Choose two.)

- A. Increase the size of the instances.
- B. Have the instance in the primary Region write the data to an Amazon SQS queue in the primary Region instead, and have the instance in the DR Region poll from this queue.
- C. Use multiple instances on the primary and DR Regions to send and receive the replication data.
- D. Change the DR Region to Oregon (us-west-2) instead of the current DR Region.
- E. Attach an additional elastic network interface to each of the instances in both Regions and set up load balancing between the network interfaces.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 320

A company has implemented AWS Organizations. It has recently set up a number of new accounts and wants to deny access to a specific set of AWS services in these new accounts.

How can this be controlled MOST efficiently?

- A. Create an IAM policy in each account that denies access to the services. Associate the policy with an IAM group, and add all IAM users to the group.
- B. Create a service control policy that denies access to the services. Add all of the new accounts to a single organizational unit (OU), and apply the policy to that OU.
- C. Create an IAM policy in each account that denies access to the services. Associate the policy with an IAM role, and instruct users to log in using their corporate credentials and assume the IAM role.

- D. Create a service control policy that denies access to the services, and apply the policy to the root of the organization.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

QUESTION 321

A company has deployed an application to multiple environments in AWS, including production and testing. The company has separate accounts for production and testing, and users are allowed to create additional application users for team members or services, as needed. The Security team has asked the Operations team for better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments.

Which of the following options would MOST securely accomplish this goal?

- A. Create a new AWS account to hold user and service accounts, such as an identity account. Create users and groups in the identity account. Create roles with appropriate permissions in the production and testing accounts. Add the identity account to the trust policies for the roles.
- B. Modify permissions in the production and testing accounts to limit creating new IAM users to members of the Operations team. Set a strong IAM password policy on each account. Create new IAM users and groups in each account to limit developer access to just the services required to complete their job function.
- C. Create a script that runs on each account that checks user accounts for adherence to a security policy. Disable any user or service accounts that do not comply.
- D. Create all user accounts in the production account. Create roles for access in the production account and testing accounts. Grant cross-account access from the production account to the testing account.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 322

A Solutions Architect must build a highly available infrastructure for a popular global video game that runs on a mobile phone platform. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The database tier is an Amazon RDS MySQL Multi-AZ instance. The entire application stack is deployed in both us-east-1 and eu-central-1. Amazon Route 53 is used to route traffic to the two installations using a latency-based routing policy. A weighted routing policy is configured in Route 53 as a fail over to another region in case the installation in a region becomes unresponsive.

During the testing of disaster recovery scenarios, after blocking access to the Amazon RDS MySQL instance in eu-central-1 from all the application instances running in that region. Route 53 does not automatically failover all traffic to us-east-1.

Based on this situation, which changes would allow the infrastructure to failover to us-east-1? (Choose two.)

- A. Specify a weight of 100 for the record pointing to the primary Application Load Balancer in us-east-1 and a weight of 60 for the pointing to the primary Application Load Balancer in eu-central-1.
- B. Specify a weight of 100 for the record pointing to the primary Application Load Balancer in us-east-1 and a weight of 0 for the record pointing to the primary Application Load Balancer in eu-central-1.
- C. Set the value of Evaluate Target Health to Yes on the latency alias resources for both eu-central-1 and us-east-1.
- D. Write a URL in the application that performs a health check on the database layer. Add it as a health

check within the weighted routing policy in both regions.

- E. Disable any existing health checks for the resources in the policies and set a weight of 0 for the records pointing to primary in both eu-central-1 and us-east-1, and set a weight of 100 for the primary Application Load Balancer only in the region that has healthy resources.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 323

An online e-commerce business is running a workload on AWS. The application architecture includes a web tier, an application tier for business logic, and a database tier for user and transactional data management. The database server has a 100 GB memory requirement. The business requires cost-efficient disaster recovery for the application with an RTO of 5 minutes and an RPO of 1 hour. The business also has a regulatory for out-of region disaster recovery with a minimum distance between the primary and alternate sites of 250 miles.

Which of the following options can the Solutions Architect design to create a comprehensive solution for this customer that meets the disaster recovery requirements?

- A. Back up the application and database data frequently and copy them to Amazon S3. Replicate the backups using S3 cross-region replication, and use AWS CloudFormation to instantiate infrastructure for disaster recovery and restore data from Amazon S3.
- B. Employ a pilot light environment in which the primary database is configured with mirroring to build a standby database on m4.large in the alternate region. Use AWS CloudFormation to instantiate the web servers, application servers and load balancers in case of a disaster to bring the application up in the alternate region. Vertically resize the database to meet the full production demands, and use Amazon Route 53 to switch traffic to the alternate region.
- C. Use a scaled-down version of the fully functional production environment in the alternate region that includes one instance of the web server, one instance of the application server, and a replicated instance of the database server in standby mode. Place the web and the application tiers in an Auto Scaling behind a load balancer, which can automatically scale when the load arrives to the application. Use Amazon Route 53 to switch traffic to the alternate region.
- D. Employ a multi-region solution with fully functional web, application, and database tiers in both regions with equivalent capacity. Activate the primary database in one region only and the standby database in the other region. Use Amazon Route 53 to automatically switch traffic from one region to another using health check routing policies.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 324

A company has a data center that must be migrated to AWS as quickly as possible. The data center has a 500 Mbps AWS Direct Connect link and a separate, fully available 1 Gbps ISP connection. A Solutions Architect must transfer 20 TB of data from the data center to an Amazon S3 bucket.

What is the FASTEST way transfer the data?

- A. Upload the data to the S3 bucket using the existing DX link.
- B. Send the data to AWS using the AWS Import/Export service.
- C. Upload the data using an 80 TB AWS Snowball device.
- D. Upload the data to the S3 bucket using S3 Transfer Acceleration.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Import/Export supports importing and exporting data into and out of Amazon S3 buckets. For significant data sets, AWS Import/Export is often faster than Internet transfer and more cost effective than upgrading your connectivity.

Reference: <https://stackshare.io/stackups/aws-direct-connect-vs-aws-import-export>

QUESTION 325

A company wants to follow its website on AWS using serverless architecture design patterns for global customers. The company has outlined its requirements as follow:

- The website should be responsive.
- The website should offer minimal latency.
- The website should be highly available.
- Users should be able to authenticate through social identity providers such as Google, Facebook, and Amazon.
- There should be baseline DDoS protections for spikes in traffic.

How can the design requirements be met?

- A. Use Amazon CloudFront with Amazon ECS for hosting the website. Use AWS Secrets Manager for provide user management and authentication functions. Use ECS Docker containers to build an API.
- B. Use Amazon Route 53 latency routing with an Application Load Balancer and AWS Fargate in different regions for hosting the website. Use Amazon Cognito to provide user management and authentication functions. Use Amazon EKS containers to build an API.
- C. Use Amazon CloudFront with Amazon S3 for hosting static web resources. Use Amazon Cognito to provide user management authentication functions. Use Amazon API Gateway with AWS Lambda to build an API.
- D. Use AWS Direct Connect with Amazon CloudFront and Amazon S3 for hosting static web resource. Use Amazon Cognito to provide user management authentication functions. Use AWS Lambda to build an API.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 326

A company runs an ordering system on AWS using Amazon SQS and AWS Lambda, with each order received as a JSON message. Recently the company had a marketing event that led to a tenfold increase in orders. With this increase, the following undesired behaviors started in the ordering system:

- Lambda failures while processing orders lead to queue backlogs.
- The same orders have been processed multiple times.

A Solutions Architect has been asked to solve the existing issues with the ordering system and add the following resiliency features:

- Retain problematic orders for analysis.
- Send notification if errors go beyond a threshold value.

How should the Solutions Architect meet these requirements?

- A. Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing, increase the visibility timeout for the messages, create a dead letter queue for messages that could not be processed, create an Amazon CloudWatch alarm on Lambda errors for notification.

- B. Receive single messages with each Lambda invocation, put additional Lambda workers to poll the queue, delete messages after processing, increase the message timer for the messages, use Amazon CloudWatch Logs for messages that could not be processed, create a CloudWatch alarm on Lambda errors for notification.
- C. Receive multiple messages with each Lambda invocation, use long polling when receiving the messages, log the errors from the message processing code using Amazon CloudWatch Logs, create a dead letter queue with AWS Lambda to capture failed invocations, create CloudWatch events on Lambda errors for notification.
- D. Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing, increase the visibility timeout for the messages, create a delay queue for messages that could not be processed, create an Amazon CloudWatch metric on Lambda errors for notification.

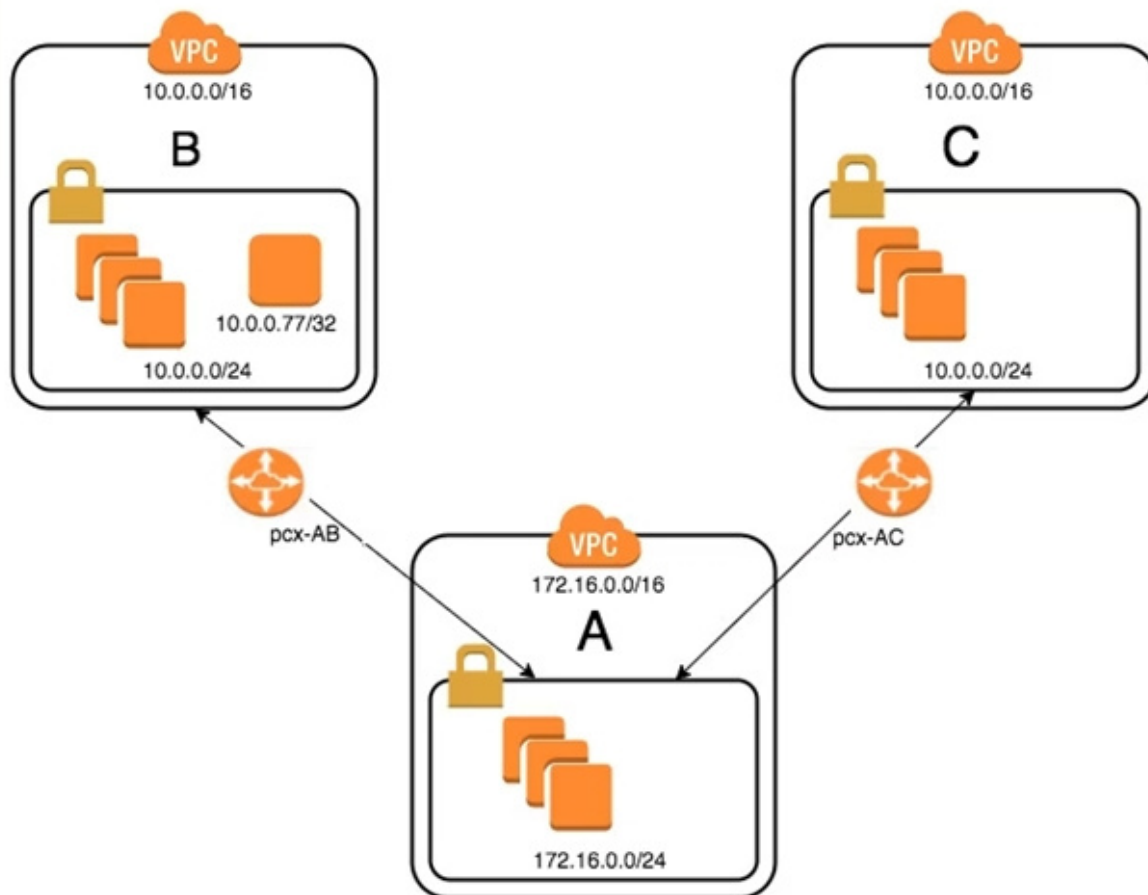
Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 327



An organization has recently grown through acquisitions. Two of the purchased companies use the same IP CIDR range. There is a new short-term requirement to allow AnyCompany A (VPC-A) to communicate with a server that has the IP address 10.0.0.77 in AnyCompany B (VPC-B). AnyCompany A must also communicate with all resources in AnyCompany C (VPC-C). The Network team has created the VPC peer links, but it is having issues with communications between VPC-A and VPC-B. After an investigation, the team believes that the routing tables in the VPCs are incorrect.

What configuration will allow AnyCompany A to communicate with AnyCompany C in addition to the database in AnyCompany B?

- A. On VPC-A, create a static route for the VPC-B CIDR range (10.0.0.0/24) across VPC peer pcx-AB.
Create a static route of 10.0.0.0/16 across VPC peer pcx-AC.
On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) on peer pcx-AB.
On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.
- B. On VPC-A, enable dynamic route propagation on pcx-AB and pcx-AC.
On VPC-B, enable dynamic route propagation and use security groups to allow only the IP address 10.0.0.77/32 on VPC peer pcx-AB.
On VPC-C, enable dynamic route propagation with VPC-A on peer pcx-AC.
- C. On VPC-A, create network access control lists that block the IP address 10.0.0.77/32 on VPC peer pcx-AC.
On VPC-A, create a static route for VPC-B CIDR (10.0.0.0/24) on pcx-AB and a static route for VPC-C CIDR (10.0.0.0/24) on pcx-AC.
On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AB.
On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.
- D. On VPC-A, create a static route for the VPC-B CIDR (10.0.0.0/24) database across VPC peer pcx-AB.
Create a static route for the VPC-C CIDR on VPC peer pcx-AC.
On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) on peer pcx-AB.
On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 328

A retail company is running an application that stores invoice files in an Amazon S3 bucket and metadata about the files in an Amazon DynamoDB table. The application software runs in both us-east-1 and eu-west-1. The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region.

Which option meets these requirements?

- A. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Enable versioning on the S3 bucket.
- B. Create an AWS Lambda function triggered by Amazon CloudWatch Events to make regular backups of the DynamoDB table. Set up S3 cross-region replication from us-east-1 to eu-west-1. Set up MFA delete on the S3 bucket in us-east-1.
- C. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable versioning on the S3 bucket. Implement strict ACLs on the S3 bucket.
- D. Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Set up S3 cross-region replication from us-east-1 to eu-west-1.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 329

A company wants to launch an online shopping website in multiple countries and must ensure that customers are protected against potential “man-in-the-middle” attacks.

Which architecture will provide the MOST secure site access?

- A. Use Amazon Route 53 for domain registration and DNS services. Enable DNSSEC for all Route 53 requests. Use AWS Certificate Manager (ACM) to register TLS/SSL certificates for the shopping website, and use Application Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all client requests to the site.

- B. Register 2048-bit encryption keys from a third-party certificate service. Use a third-party DNS provider that uses the customer managed keys for DNSSEC. Upload the keys to ACM, and use ACM to automatically deploy the certificates for secure web services to an EC2 front-end web server fleet by using NGINX. Use the Server Name Identification extension in all client requests to the site.
- C. Use Route 53 for domain registration. Register 2048-bit encryption keys from a third-party certificate service. Use a third-party DNS service that supports DNSSEC for DNS requests that use the customer managed keys. Import the customer managed keys to ACM to deploy the certificates to Classic Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all clients requests to the site.
- D. Use Route 53 for domain registration, and host the company DNS root servers on Amazon EC2 instances running `Bind.Enable DNSSEC` for DNS requests. Use ACM to register TLS/SSL certificates for the shopping website, and use Application Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all client requests to the site.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 330

A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle of least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes.

Which account creation process meets these requirements and allows for changes?

- A. Create a new AWS Organizations account. Create groups in Active Directory and assign them to roles in AWS to grant federated access. Require each team to tag their resources, and separate bills based on tags. Control access to resources through IAM granting the minimally required privilege.
- B. Create individual accounts for each team. Assign the security account as the master account, and enable consolidated billing for all other accounts. Create a cross-account role for security to manage accounts, and send logs to a bucket in the security account.
- C. Create a new AWS account, and use AWS Service Catalog to provide teams with the required resources. Implement a third-party billing solution to provide the Finance team with the resource use for each team based on tagging. Isolate resources using IAM to avoid account sprawl. Security will control and monitor logs and permissions.
- D. Create a master account for billing using Organizations, and create each team's account from that master account. Create a security account for logs and cross-account access. Apply service control policies on each account, and grant the Security team cross-account access to all accounts. Security will create IAM policies for each account to maintain least privilege access.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions anytime. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)

Reference: <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

QUESTION 331

A company has a 24 TB MySQL database in its on-premises data center that grows at the rate of 10 GB per day. The data center is connected to the company's AWS infrastructure with a 50 Mbps VPN connection.

The company is migrating the application and workload to AWS. The application code is already installed and tested on Amazon EC2. The company now needs to migrate the database and wants to go live on AWS within 3 weeks.

Which of the following approaches meets the schedule with LEAST downtime?

- A.
 1. Use the VM Import/Export service to import a snapshot of the on-premises database into AWS.
 2. Launch a new EC2 instance from the snapshot.
 3. Set up ongoing database replication from on premises to the EC2 database over the VPN.
 4. Change the DNS entry to point to the EC2 database.
 5. Stop the replication.
- B.
 1. Launch an AWS DMS instance.
 2. Launch an Amazon RDS Aurora MySQL DB instance.
 3. Configure the AWS DMS instance with on-premises and Amazon RDS MySQL database information.
 4. Start the replication task within AWS DMS over the VPN.
 5. Change the DNS entry to point to the Amazon RDS MySQL database.
 6. Stop the replication.
- C.
 1. Create a database export locally using database-native tools.
 2. Import that into AWS using AWS Snowball.
 3. Launch an Amazon RDS Aurora DB instance.
 4. Load the data in the RDS Aurora DB instance from the export.
 5. Set up database replication from the on-premises database to the RDS Aurora DB instance over the VPN.
 6. Change the DNS entry to point to the RDS Aurora DB instance.
 7. Stop the replication.
- D.
 1. Take the on-premises application offline.
 2. Create a database export locally using database-native tools.
 3. Import that into AWS using AWS Snowball.
 4. Launch an Amazon RDS Aurora DB instance.
 5. Load the data in the RDS Aurora DB instance from the export.
 6. Change the DNS entry to point to the Amazon RDS Aurora DB instance.
 7. Put the Amazon EC2 hosted application online.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 332

A company wants to allow its Marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The Team Manager must have the ability to manage users and groups, but no team members should have access to services or resources not required for the SQL queries. Additionally, Administrators need to audit the queries made and receive notifications when a query violates rules defined by the Security team.

AWS Organizations has been used to create a new account and an AWS IAM user with administrator permissions for the Team Manager.

Which design meets these requirements?

- A. Apply a service control policy (SCP) that allows access to IAM, Amazon RDS, and AWS CloudTrail. Load customer records in Amazon RDS MySQL and train users to execute queries using the AWS CLI. Stream the query logs to Amazon CloudWatch Logs from the RDS database instance. Use a subscription filter with AWS Lambda functions to audit and alarm on queries against personal data.
- B. Apply a service control policy (SCP) that denies access to all services except IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer record files in Amazon S3 and train users to execute queries using the CLI via Athena. Analyze CloudTrail events to audit and alarm on queries against personal data.

- C. Apply a service control policy (SCP) that denies access to all services except IAM, Amazon DynamoDB, and AWS CloudTrail. Store customer records in DynamoDB and train users to execute queries using the AWS CLI. Enable DynamoDB streams to track the queries that are issued and use an AWS Lambda function for real-time monitoring and alerting.
- D. Apply a service control policy (SCP) that allows access to IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer records as files in Amazon S3 and train users to leverage the Amazon S3 Select feature and execute queries using the AWS CLI. Enable S3 object-level logging and analyze CloudTrail events to audit and alarm on queries against personal data.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 333

A Solutions Architect is responsible for redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high-memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds them to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them, and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average, most of which is spent waiting on external service calls, but the application is written to process multiple items in parallel.

Traffic to this service is unpredictable. During periods of high load, items may sit in the internal queue for over an hour while the application processes the backlog. In addition, the current system has issues with availability and data loss if the single application node fails.

Clients that access this service cannot be modified. They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request.

Which approach would improve the availability and durability of the system while decreasing the processing latency and minimizing costs?

- A. Create an Amazon API Gateway REST API that uses Lambda proxy integration to pass requests to an AWS Lambda function. Migrate the core processing code to a Lambda function and write a wrapper class that provides a handler method that converts the proxy events to the internal application data model and invokes the processing module.
- B. Create an Amazon API Gateway REST API that uses a service proxy to put items in an Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS instead of an in-memory queue. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SQS queue.
- C. Modify the application to use Amazon DynamoDB instead of Amazon RDS. Configure Auto Scaling for the DynamoDB table. Deploy the application within an Auto Scaling group with a scaling policy based on CPU utilization. Back the in-memory queue with a memory-mapped file to an instance store volume and periodically write that file to Amazon S3.
- D. Update the application to use a Redis task queue instead of the in-memory queue. Build a Docker container image for the application. Create an Amazon ECS task definition that includes the application container and a separate container to host Redis. Deploy the new task definition as an ECS service using AWS Fargate, and enable Auto Scaling.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 334

A company has an internal AWS Elastic Beanstalk worker environment inside a VPC that must access an external payment gateway API available on an HTTPS endpoint on the public internet. Because of security policies, the payment gateway's Application team can grant access to only one public IP address.

Which architecture will set up an Elastic Beanstalk environment to access the company's application without making multiple changes on the company's end?

- A. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet with an outbound route to a NAT gateway in a public subnet. Associate an Elastic IP address to the NAT gateway that can be whitelisted on the payment gateway application side.
- B. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet with an internet gateway. Associate an Elastic IP address to the internet gateway that can be whitelisted on the payment gateway application side.
- C. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet. Set an `HTTPS_PROXY` application parameter to send outbound HTTPS connections to an EC2 proxy server deployed in a public subnet. Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side.
- D. Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet. Set the `HTTPS_PROXY` and `NO_PROXY` application parameters to send non-VPC outbound HTTPS connections to an EC2 proxy server deployed in a public subnet. Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/vpc.html>

QUESTION 335

A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The Quality Assurance (QA) department needs to launch a large number of short-lived environments to test the application. The application environments are currently launched by the Manager of the department using an AWS CloudFormation template. To launch the stack, the Manager uses a role with permission to use CloudFormation, EC2, and Auto Scaling APIs. The Manager wants to allow testers to launch their own environments, but does not want to grant broad permissions to each user.

Which set up would achieve these goals?

- A. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the Manager's role and add a policy that restricts the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.
- B. Create an AWS Service Catalog product from the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the template from the AWS Service Catalog console.
- C. Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.
- D. Create an AWS Elastic Beanstalk application from the environment template. Give users in the QA department permission to use Elastic Beanstalk permissions only. Train users to launch Elastic Beanstalk CLI, passing the existing role to the environment as a service role.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 336

A company has several teams, and each team has their own Amazon RDS database that totals 100 TB. The company is building a data query platform for Business Intelligence Analysts to generate a weekly

business report: The new system must run ad-hoc SQL queries.

What is the MOST cost-effective solution?

- A. Create a new Amazon Redshift cluster. Create an AWS Glue ETL job to copy data from the RDS databases to the Amazon Redshift cluster. Use Amazon Redshift to run the query.
- B. Create an Amazon EMR cluster with enough core nodes. Run an Apache Spark job to copy data from the RDS databases to a Hadoop Distributed File System (HDFS). Use a local Apache Hive metastore to maintain the table definition. Use Spark SQL to run the query.
- C. Use an AWS Glue ETL job to copy all the RDS databases to a single Amazon Aurora PostgreSQL database. Run SQL queries on the Aurora PostgreSQL database.
- D. Use an AWS Glue crawler to crawl all the databases and create tables in the AWS Glue Data Catalog. Use an AWS Glue ETL job to load data from the RDS databases to Amazon S3, and use Amazon Athena to run the queries.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 337

A company provides AWS solutions to its users with AWS CloudFormation templates. Users launch the templates in their accounts to have different solutions provisioned for them. The users want to improve the deployment strategy for solutions while retaining the ability to do the following:

- Add their own features to a solution for their specific deployments.
- Run unit tests on their changes.
- Turn features on and off for their deployments.
- Automatically update with code changes.
- Run security scanning tools for their deployments.

Which strategies should the Solutions Architect use to meet the requirements?

- A. Allow users to download solution code as Docker images. Use AWS CodeBuild and AWS CodePipeline for the CI/CD pipeline. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use AWS CodeDeploy to run unit tests and security scans, and for deploying and updating a solution with changes.
- B. Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use AWS Amplify plugins for different solution features and user prompts to turn features on and off. Use AWS Lambda to run unit tests and security scans, and AWS CodeBuild for deploying and updating a solution with changes.
- C. Allow users to download solution code artifacts in their Amazon S3 buckets. Use Amazon S3 and AWS CodePipeline for the CI/CD pipelines. Use CloudFormation StackSets for different solution features and to turn features on and off. Use AWS Lambda to run unit tests and security scans, and CloudFormation for deploying and updating a solution with changes.
- D. Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use the AWS Cloud Development Kit constructs for different solution features, and use the manifest file to turn features on and off. Use AWS CodeBuild to run unit tests and security scans, and for deploying and updating a solution with changes.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.slideshare.net/AmazonWebServices/cicd-for-containers-a-way-forward-for-your-devops-pipeline>

QUESTION 338

A fleet of Amazon ECS instances is used to poll an Amazon SQS queue and update items in an Amazon

DynamoDB database. Items in the table are not being updated, and the SQS queue is filling up. Amazon CloudWatch Logs are showing consistent 400 errors when attempting to update the table. The provisioned write capacity units are appropriately configured, and no throttling is occurring.

What is the LIKELY cause of the failure?

- A. The ECS service was deleted.
- B. The ECS configuration does not contain an Auto Scaling group.
- C. The ECS instance task execution IAM role was modified.
- D. The ECS task role was modified.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 339

A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content. The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB.

What can a Solutions Architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

- A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 `PutObject` operation. Secure the API Gateway using a `COGNITO_USER_POOLS` authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 `PutObject` operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload API objects.
- C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload API.
- D. Configure an Amazon CloudFront distribution for the destination S3 bucket. Enable PUT and POST methods for the CloudFront cache behavior. Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user `s3:PutObject` permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 340

A company's CISO has asked a Solutions Architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its application can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.

The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer. The company is currently using GitHub to host the application source code, and has configured an AWS CodeBuild project to build the application. The company also intends to use AWS CodePipeline to trigger builds from GitHub commits using the existing CodeBuild project.

What CI/CD configuration meets all of the requirements?

- A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update.
- B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.
- C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update.
- D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 341

A company wants to analyze log data using date ranges with a custom application running on AWS. The application generates about 10 GB of data every day, which is expected to grow. A Solutions Architect is tasked with storing the data in Amazon S3 and using Amazon Athena to analyze the data.

Which combination of steps will ensure optimal performance as the data grows? (Choose two.)

- A. Store each object in Amazon S3 with a random string at the front of each key.
- B. Store the data in multiple S3 buckets.
- C. Store the data in Amazon S3 in a columnar format, such as Apache Parquet or Apache ORC.
- D. Store the data in Amazon S3 in objects that are smaller than 10 MB.
- E. Store the data using Apache Hive partitioning in Amazon S3 using a key that includes a date, such as dt=2019-02.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 342

An advisory firm is creating a secure data analytics solution for its regulated financial services users. Users will upload their raw data to an Amazon S3 bucket, where they have PutObject permissions only. Data will be analyzed by applications running on an Amazon EMR cluster launched in a VPC. The firm requires that the environment be isolated from the internet. All data at rest must be encrypted using keys controlled by the firm.

Which combination of actions should the Solutions Architect take to meet the user's security requirements? (Choose two.)

- A. Launch the Amazon EMR cluster in a private subnet configured to use an AWS KMS CMK for at-rest encryption. Configure a gateway VPC endpoint for Amazon S3 and an interface VPC endpoint for AWS KMS.
- B. Launch the Amazon EMR cluster in a private subnet configured to use an AWS KMS CMK for at-rest encryption. Configure a gateway VPC endpoint for Amazon S3 and a NAT gateway to access AWS KMS.
- C. Launch the Amazon EMR cluster in a private subnet configured to use an AWS CloudHSM appliance for at-rest encryption. Configure a gateway VPC endpoint for Amazon S3 and an interface VPC endpoint for CloudHSM.
- D. Configure the S3 endpoint policies to permit access to the necessary data buckets only.

- E. Configure the S3 bucket policies to permit access using an `aws:sourceVpce` condition to match the S3 endpoint ID.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 343

While debugging a backend application for an IoT system that supports globally distributed devices, a Solutions Architect notices that stale data is occasionally being sent to user devices. Devices often share data, and stale data does not cause issues in most cases. However, device operations are disrupted when a device reads the stale data after an update.

The global system has multiple identical application stacks deployed in different AWS Regions. If a user device travels out of its home geographic region, it will always connect to the geographically closest AWS Region to write or read data. The same data is available in all supported AWS Regions using an Amazon DynamoDB global table.

What change should be made to avoid causing disruptions in device operations?

- A. Update the backend to use strongly consistent reads. Update the devices to always write to and read from their home AWS Region.
- B. Enable strong consistency globally on a DynamoDB global table. Update the backend to use strongly consistent reads.
- C. Switch the backend data store to Amazon Aurora MySQL with cross-region replicas. Update the backend to always write to the master endpoint.
- D. Select one AWS Region as a master and perform all writes in that AWS Region only. Update the backend to use strongly consistent reads.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 344

A software as a service (SaaS) company offers a cloud solution for document management to private law firms and the public sector. A local government client recently mandated that highly confidential documents cannot be stored outside the country. The company CIO asks a Solutions Architect to ensure the application can adapt to this new requirement. The CIO also wants to have a proper backup plan for these documents, as backups are not currently performed.

What solution meets these requirements?

- A. Tag documents that are not highly confidential as regular in Amazon S3. Create individual S3 buckets for each user. Upload objects to each user's bucket. Set S3 bucket replication from these buckets to a central S3 bucket in a different AWS account and AWS Region. Configure an AWS Lambda function triggered by scheduled events in Amazon CloudWatch to delete objects that are tagged as secret in the S3 backup bucket.
- B. Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Create a cross-region S3 bucket in a separate AWS account. Set proper IAM roles to allow cross-region permissions to the S3 buckets. Configure an AWS Lambda function triggered by Amazon CloudWatch scheduled events to copy objects that are tagged as secret to the S3 backup bucket and objects tagged as cross-region S3 bucket.
- C. Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to an S3 bucket in a different AWS Region. Configure an AWS Lambda function that triggers when new S3 objects are created in the main bucket to replicate only documents

tagged as secret into the S3 bucket in the same AWS Region.

- D. Tag highly confidential documents as secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to an S3 bucket in a different AWS Region. Create an Amazon CloudWatch Events rule for new S3 objects tagged as secret to trigger an AWS Lambda function to replicate them into a separate bucket in the same AWS Region.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 345

A company is having issues with a newly deployed serverless infrastructure that uses Amazon API Gateway, Amazon Lambda, and Amazon DynamoDB.

In a steady state, the application performs as expected. However, during peak load, tens of thousands of simultaneous invocations are needed and user requests fail multiple times before succeeding. The company has checked the logs for each component, focusing specifically on Amazon CloudWatch Logs for Lambda. There are no errors logged by the services or applications.

What might cause this problem?

- A. Lambda has very low memory assigned, which causes the function to fail at peak load.
- B. Lambda is in a subnet that uses a NAT gateway to reach out of the internet, and the function instance does not have sufficient Amazon EC2 resources in the VPC to scale with the load.
- C. The throttle limit set on API Gateway is very low. During peak load, the additional requests are not making their way through to Lambda.
- D. DynamoDB is set up in an auto scaling mode. During peak load, DynamoDB adjusts capacity and throughput behind the scenes, which is causing the temporary downtime. Once the scaling completes, the retries go through successfully.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html>

QUESTION 346

A large company with hundreds of AWS accounts has a newly established centralized internal process for purchasing new or modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement or execution. Previously, business units would directly purchase or modify Reserved Instances in their own respective AWS accounts autonomously.

Which combination of steps should be taken to proactively enforce the new process in the MOST secure way possible? (Choose two.)

- A. Ensure all AWS accounts are part of an AWS Organizations structure operating in all features mode.
- B. Use AWS Config to report on the attachment of an IAM policy that denies access to the `ec2:PurchaseReservedInstancesOffering` and `ec2:ModifyReservedInstances` actions.
- C. In each AWS account, create an IAM policy with a DENY rule to the `ec2:PurchaseReservedInstancesOffering` and `ec2:ModifyReservedInstances` actions.
- D. Create an SCP that contains a deny rule to the `ec2:PurchaseReservedInstancesOffering` and `ec2:ModifyReservedInstances` actions. Attach the SCP to each organizational unit (OU) of the AWS Organizations structure.
- E. Ensure that all AWS accounts are part of an AWS Organizations structure operating in consolidated

billing features mode.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 347

A Solutions Architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint. The Solutions Architect wants an end-to-end view of each request to analyze the latency of the request and create service maps.

How can the Solutions Architect design the API Gateway access control and perform request inspections?

- A. For the API Gateway method, set the authorization to AWS_IAM. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Enable the API caller to sign requests with AWS Signature when accessing the endpoint. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- B. For the API Gateway resource, set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.
- C. Create an AWS Lambda function as the custom authorizer, ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- D. Create a client certificate for API Gateway. Distribute the certificate to the AWS users and roles that need to access the endpoint. Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-cors.html>

QUESTION 348

A Solutions Architect needs to design a highly available application that will allow authenticated users to stay connected to the application even when there are underlying failures.

Which solution will meet these requirements?

- A. Deploy the application on Amazon EC2 instances. Use Amazon Route 53 to forward requests to the EC2 instances. Use Amazon DynamoDB to save the authenticated connection details.
- B. Deploy the application on Amazon EC2 instances in an Auto Scaling group. Use an internet-facing Application Load Balancer to handle requests. Use Amazon DynamoDB to save the authenticated connection details.
- C. Deploy the application on Amazon EC2 instances in an Auto Scaling group. Use an internet-facing Application Load Balancer on the front end. Use EC2 instances to save the authenticated connection details.
- D. Deploy the application on Amazon EC2 instances in an Auto Scaling group. Use an internet-facing Application Load Balancer on the front end. Use EC2 instances hosting a MySQL database to save the authenticated connection details.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 349

An enterprise company wants to implement cost controls for all its accounts in AWS Organizations, which has full features enabled. The company has mapped organizational units (OUs) to its business units, and it wants to bill these business units for their individual AWS spending. There has been a recent spike in the company's AWS bill, which is generating attention from the Finance team. A Solutions Architect needs to investigate the cause of the spike while designing a solution that will track AWS costs in Organizations and generate a notification to the required teams if costs from a business unit exceed a specific monetary threshold.

Which solution will meet these requirements?

- A. Use Cost Explorer to troubleshoot the reason for the additional costs. Set up an AWS Lambda function to monitor the company's AWS bill by each AWS account in an OU. Store the threshold amount set by the Finance team in the AWS Systems Manager Parameter Store. Write the custom rules in the Lambda function to verify any hidden costs for the AWS accounts. Trigger a notification from the Lambda function to an Amazon SNS topic when a budget threshold is breached.
- B. Use AWS Trusted Advisor to troubleshoot the reason for the additional costs. Set up an AWS Lambda function to monitor the company's AWS bill by each AWS account in an OU. Store the threshold amount set by the Finance team in the AWS Systems Manager Parameter Store. Write custom rules in the Lambda function to verify any hidden costs for the AWS accounts. Trigger an email to the required teams from the Lambda function using Amazon SNS when a budget threshold is breached.
- C. Use Cost Explorer to troubleshoot the reason for the additional costs. Create a budget using AWS Budgets with the monetary amount set by the Finance team for each OU by grouping the linked accounts. Configure an Amazon SNS notification to the required teams in the budget.
- D. Use AWS Trusted Advisor to troubleshoot the reason for the additional costs. Create a budget using AWS Budgets with the monetary amount set by the Finance team for each OU by grouping the linked accounts. Add the Amazon EC2 instance types to be used in the company as a budget filter. Configure an Amazon SNS topic with a subscription for the Finance team email address to receive budget notifications.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference: