ULTIMATE Q/A AWS SAP-C01

Solutions Architect Professional

Questions

Luca Cesarano
https://lucacesarano.com

Table of Contents

Questions 390-399

Question #390

As a result, one of your AWS Data Pipeline operations failed and reached a hard failure state after three retries.
You want to attempt it once again.

Can the number of automated retries be increased to more than three?

- 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.

Commented [LC1]: 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.
Reference:
https://aws.amazon.com/datapipeline/faqs/

Question #391 (EXAM)

A business is arranging connection to a multi-account AWS environment in order to handle application workloads serving a single geographic region's users. The workloads are dependent on an on-premises legacy system that is highly available and distributed over two sites. Connectivity to the legacy system is important for the AWS workloads, and a minimum of 5 Gbps of bandwidth is needed. All AWS application workloads must be connected to one another.

Which solution will satisfy these criteria?

- A. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from a DX partner for each on-premises location. Create private virtual interfaces on each connection for each AWS account VPC. Associate the private virtual interface with a virtual private gateway attached to each VPC.
- B. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location. Create and attach a virtual private gateway for each AWS account VPC. Create a DX gateway in a central network account and associate it with the virtual private gateways. Create a public virtual interface on each DX connection and associate the interface with the DX gateway.
- C. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location. Create a transit gateway and a DX gateway in a central network account. Create a transit virtual interface for each DX interface and associate them with the DX gateway. Create a gateway association between the DX gateway and the transit gateway.
- D. Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from a DX partner for each on-premises location. Create and attach a virtual private gateway for each AWS account VPC. Create a transit gateway in a central network account and associate it with the virtual private gateways. Create a transit virtual interface on each DX connection and attach the interface to the transit gateway.

Commented [LC2]: A - no, there is no connection between VPCs.

B - no, bcz DX gateway doesn't support routing from one VPN to another

Ref.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

C - right answer.
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

D - no, you can not connect Direct Connect to the Transit gateway without Direct Connect gateway in the middle.

Question #392

A Solutions Architect is tasked with the responsibility of migrating an existing on-premises web application that contains 70 TB of static files and is used to support a public open-data project. As part of the migration process, the Architect want to update to the newest version of the host operating system.

Which method of migration is the FASTEST and MOST cost-effective?

- 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.

Commented [LC3]: C
A: This will be too slow.
B: Direct connect takes too long to provision.
C: Because the question did not state what is the bandwidth of the company, using Snowball to transfer 70TB make sense.
D: While this is possible, we do not know If the server is physical or virtual and SMS just migrate it does not upgrade. Wherelse in C you can immediately select the best AMI to start and rely on Snowball to transfer the data.

Question #393

A firm intends to migrate regulated and security-sensitive operations to AWS. The Security team is establishing a framework to ensure that AWS best practices and industry-recognized compliance requirements are being followed. For teams, the AWS Management Console is the primary way of resource provisioning.

Which tactics should a Solutions Architect use to ensure that business needs are met and that the configurations of AWS resources are regularly assessed, audited, and monitored? (Select two.)

- A. Use AWS Config rules to periodically audit changes to AWS resources and monitor the compliance of the configuration. Develop AWS Config custom rules using AWS Lambda to establish a test-driven development approach, and further automate the evaluation of configuration changes against the required controls.
- B. Use Amazon CloudWatch Logs agent to collect all the AWS SDK logs. Search the log data using a pre-defined set of filter patterns that matches mutating API calls. Send notifications using Amazon CloudWatch alarms when unintended changes are performed. Archive log data by using a batch export to Amazon S3 and then Amazon Glacier for a long-term retention and auditability.
- C. Use AWS CloudTrail events to assess management activities of all AWS accounts. Ensure that CloudTrail is enabled in all accounts and available AWS services. Enable trails, encrypt CloudTrail event log files with an AWS KMS key, and monitor recorded activities with CloudWatch Logs.
- D. Use the Amazon CloudWatch Events near-real-time capabilities to monitor system events patterns, and trigger AWS Lambda functions to automatically revert non-authorized changes in AWS resources. Also, target Amazon SNS topics to enable notifications and improve the response time of incident responses.
- E. Use CloudTrail integration with Amazon SNS to automatically notify unauthorized API activities. Ensure that CloudTrail is enabled in all accounts and available AWS services. Evaluate the usage of Lambda functions to automatically revert non-authorized changes in AWS resources.

Commented [LC4]: My answers are "A & C".
The key point in the question is that it request to "asses, audit & monitor". Therefore, any answer that contains terminations for instances/services shall be eliminated.
So, "D & E": are out because they are taking actions.
"B": does not make sense!
A: Config rules, are very useful tool for compliancy.
C: Cloud Trail is also great tool for auditing.

Commented [LC5]:

Question #394

A business is building a new service that will be accessible through TCP on a fixed port. A solutions architect must guarantee that the service is highly available, redundant across Availability Zones, and reachable through the publicly accessible DNS name my.service.com. The service must use fixed address assignments in order for other businesses to add the addresses to their allow list.

Which solution will fulfill these criteria if resources are distributed across several Availability Zones within a single Region?

- A. Create Amazon EC2 instances with an Elastic IP address for each instance. Create a Network Load Balancer (NLB) and expose the static TCP port. Register EC2 instances with the NLB. Create a new name server record set named my.service.com, and assign the Elastic IP addresses of the EC2 instances to the record set. Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists.
- B. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP addresses for the ECS cluster. Create a Network Load Balancer (NLB) and expose the TCP port. Create a target group and assign the ECS cluster name to the NLB. Create a new A record set named my.service.com, and assign the public IP addresses of the ECS cluster to the record set. Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.
- C. Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone. Create a Network Load Balancer (NLB) and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone. Create a target group and register the EC2 instances with the NLB. Create a new A (alias) record set named my.service.com, and assign the NLB DNS name to the record set.
- D. Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP address for each host in the cluster. Create an Application Load Balancer (ALB) and expose the static TCP port. Create a target group and assign the ECS service definition name to the ALB. Create a new CNAME record set and associate the public IP addresses to the record set. Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists.

Commented [LC6]: Answer is C most probably. In A, B and D, ELB is created but Route53 never uses that as the resource in the A-record, instead routes traffic directly to the underlying EC2 or ECS instances. However, there is no mention of providing Elastic IP addresses of the EC2 instances to the external services that will use them for whitelisting. So I am a bit confused.

Question #395

A business must establish a centralized logging infrastructure for all of its Amazon Web Services accounts. The architecture should provide near-real-time data analysis across all AWS CloudTrail and VPC Flow logs. The organization intends to analyze logs in the logging account using Amazon Elasticsearch Service (Amazon ES).

Which method should a solutions architect use in order to satisfy these requirements?

- A. Configure CloudTrail and VPC Flow Logs in each AWS account to send data to a centralized Amazon S3 bucket in the logging account. Create an AWS Lambda function to load data from the S3 bucket to Amazon ES in the logging account.
- B. Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch account. Configure a CloudWatch subscription filter in each AWS account to send data to Amazon Kinesis Data Firehouse in the logging account. Load data from Kinesis Data Firehouse into Amazon ES in the logging account.
- C. Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket in each AWS account. Create an AWS Lambda function triggered by S3 events to copy the data to a centralized logging bucket. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.
- D. Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch Logs in each AWS account. Create AWS Lambda functions in each AWS accounts to subscribe to the log groups and stream the data to an Amazon S3 bucket in the logging account. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.

Commented [LC7]: B is correct.

Cross-account log data sharing using Kinesis Data Firehose with a destionation set to Amazon ES
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CrossAccountSubscriptions-Firehose.html

Question #396

A solutions architect must assess a business's Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to determine how effectively the business is using resources. The organization uses numerous big, high-memory Amazon EC2 instances to host database clusters in active/passive setups. The organization has not detected a pattern in how these EC2 instances are used by the apps that access the databases. The solutions architect must conduct an analysis of the environment and take appropriate action depending on the results.

Which option best fits these criteria in terms of cost-effectiveness?

- A. Create a dashboard by using AWS Systems Manager OpsCenter. Configure visualizations for Amazon CloudWatch metrics that are associated with the EC2 instances and their EBS volumes. Review the dashboard periodically, and identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- B. Turn on Amazon CloudWatch detailed monitoring for the EC2 instances and their EBS volumes. Create and review a dashboard that is based on the metrics. Identify usage patterns. Rightsize the EC2 instances based on the peaks in the metrics.
- C. Install the Amazon CloudWatch agent on each of the EC2 instances. Turn on AWS Compute Optimizer, and let it run for at least 12 hours. Review the recommendations from Compute Optimizer, and rightsize the EC2 instances as directed.
- D. Sign up for the AWS Enterprise Support plan. Turn on AWS Trusted Advisor. Wait 12 hours. Review the recommendations from Trusted Advisor, and rightsize the EC2 instances as directed.

Commented [LC8]: https://aws.amazon.com/compute-optimizer/

Question #397

On-premises, a business runs a high-volume media-sharing program. It presently stores over 400 terabytes of data, including millions of video clips. The organization is transferring this application to AWS in order to increase the application's stability and save expenses.
The Solutions Architecture team intends to store the films in an Amazon S3 bucket and distribute them to customers using Amazon CloudFront. The organization needs to transition this application to AWS within ten days with minimal downtime. Currently, the firm has a 1 Gbps connection to the Internet, with 30% of available capacity.

Which of the following options would allow the organization to shift the workload to AWS while remaining compliant with all requirements?

- A. Use a multi-part upload in Amazon S3 client to parallel-upload the data to the Amazon S3 bucket over the Internet. Use the throttling feature to ensure that the Amazon S3 client does not use more than 30 percent of available Internet capacity.
- B. Request an AWS Snowmobile with 1 PB capacity to be delivered to the data center. Load the data into Snowmobile and send it back to have AWS download that data to the Amazon S3 bucket. Sync the new data that was generated while migration was in flight.
- C. Use an Amazon S3 client to transfer data from the data center to the Amazon S3 bucket over the Internet. Use the throttling feature to ensure the Amazon S3 client does not use more than 30 percent of available Internet capacity.
- D. Request multiple AWS Snowball devices to be delivered to the data center. Load the data concurrently into these devices and send it back. Have AWS download that data to the Amazon S3 bucket. Sync the new data that was generated while migration was in flight.

Commented [LC9]: How should I choose between Snowmobile and Snowball?

To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball. In addition, you should evaluate the amount of available bandwidth in your network backbone. If you have a high speed backbone with hundreds of Gb/s of spare throughput, then you can use Snowmobile to migrate the large datasets all at once. If you have limited bandwidth on your backbone, you should consider using multiple Snowballs to migrate the data incrementally.

Question #398

On AWS, a business is developing a new highly accessible web application. The application needs constant and dependable communication between its AWS application servers and a backend REST API housed on-premises. The backend connection between AWS and on-premises will be handled over a private virtual interface using an AWS Direct Connect connection. Amazon Route 53 will be utilized to handle the application's private DNS records for resolving the IP address for the backend REST API.

Which architecture would be most likely to establish a secure connection to the backend API?

- A. Implement at least two backend endpoints for the backend REST API, and use Route 53 health checks to monitor the availability of each backend endpoint and perform DNS-level failover.
- B. Install a second Direct Connect connection from a different network carrier and attach it to the same virtual private gateway as the first Direct Connect connection.
- C. Install a second cross connect for the same Direct Connect connection from the same network carrier, and join both connections to the same link aggregation group (LAG) on the same private virtual interface.
- D. Create an IPSec VPN connection routed over the public internet from the on-premises data center to AWS and attach it to the same virtual private gateway as the Direct Connect connection.

Commented [LC10]: https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html

Question #399

A business is distributing both static and dynamic content from a web application operating behind an Application Load Balancer through an Amazon CloudFront distribution. For dynamic content, the web application needs user authorisation and session monitoring. The CloudFront distribution is set with a single cache behavior that forwards the HTTP whitelist headers Authorization, Host, and User-Agent, as well as a session cookie, to the origin. All other cache behavior parameters are left alone.
A valid ACM certificate is deployed to the CloudFront distribution through the distribution settings, along with a corresponding CNAME. Additionally, the ACM certificate is applied to the Application Load Balancer's HTTPS listener. CloudFront's origin protocol policy is configured to use exclusively HTTPS. According to the cache statistics report, this distribution has an extremely high miss rate.

What can the Solutions Architect do to increase this distribution's cache hit rate without jeopardizing the SSL/TLS handshake between CloudFront and the Application Load Balancer?

- A. Create two cache behaviors for static and dynamic content. Remove the User-Agent and Host HTTP headers from the whitelist headers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content.
- B. Remove the User-Agent and Authorization HTTP headers from the whitelist headers section of the cache behavior. Then update the cache behavior to use presigned cookies for authorization.
- C. Remove the Host HTTP header from the whitelist headers section and remove the session cookie from the whitelist cookies section for the default cache behavior. Enable automatic object compression and use Lambda@Edge viewer request events for user authorization.
- D. Create two cache behaviors for static and dynamic content. Remove the User-Agent HTTP header from the whitelist headers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content.

Commented [LC11]: Correct Answer - D
Since it's distribution both Static & Dynamic content. You should have two cache behaviors. So Option B & C is eliminated. Now between A & D, Host HTTP headers is required, and you can't remove. So only Valid Option is D
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/understanding-the-cache-key.html

Questions 400-499

Question #400

A user has configured the IAM policy to deny any requests that do not originate from IP 10.10.10.1/32. The other regulation is that all requests must be made between 5 and 7 p.m.

What happens at 6 p.m. if a user requests access from IP 55.109.10.12/32?

- A. It will deny access
- B. It is not possible to set a policy based on the time or IP
- C. IAM will throw an error for policy conflict
- D. It will allow access

Commented [LC12]: When a request is made, the AWS IAM policy decides whether a given request should be allowed or denied. The evaluation logic follows these rules:
By default, all requests are denied. (In general, requests made using the account credentials for resources in the account are always allowed.)
An explicit allow policy overrides this default. An explicit deny policy overrides any allows.
In this case since there are explicit deny and explicit allow statements. Thus, the request will be denied since deny overrides allow.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

Question #401

A business operates an application that is spread over many Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. All application access attempts must be made accessible for examination to the security team. The IP address of the client, the kind of connection, and the user agent must all be supplied.

Which solution will satisfy these criteria?

- A. Enable EC2 detailed monitoring, and include network logs. Send all logs through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis.
- B. Enable VPC Flow Logs for all EC2 instance network interfaces. Publish VPC Flow Logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs.
- C. Enable access logs for the Application Load Balancer, and publish the logs to an Amazon S3 bucket. Have the security team use Amazon Athena to query and analyze the logs.
- D. Enable Traffic Mirroring and specify all EC2 instance network interfaces as the source. Send all traffic information through Amazon Kinesis Data Firehose to an Amazon Elasticsearch Service (Amazon ES) cluster that the security team uses for analysis.

Commented [LC13]:

Question #402

You are responsible for a web application that utilizes an Elastic Load Balancing (ELB) load balancer in front of an Amazon Elastic Compute Cloud (EC2) Auto Scaling group of instances. A new Amazon Machine Image (AMI) was built for a recent deployment of a new version of the application, and the Auto Scaling group was modified with a new launch configuration that references the new AMI. You got reports from users throughout the rollout that the website was responding incorrectly. All occurrences were found to be in good health by the ELB.

What should you do to ensure that future deployments are error-free? (Select 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.

Commented [LC14]:

Commented [LC15]:

Question #403

A business is expanding its permitted external vendor base to include solely IPv6 connection. The company's backend systems are located inside an Amazon VPC's private subnet. The organization utilizes a NAT gateway to facilitate communication between these systems and external suppliers through IPv4. According to company policy, systems that connect with external vendors must be protected by a security group that restricts access to only authorized external suppliers. The virtual private cloud (VPC) makes use of the default network access control list (ACL).

Each backend system is successfully assigned IPv6 addresses by the Systems Operator. Additionally, the Systems Operator modifies the outgoing security group to include the external vendor's IPv6 CIDR (destination). The computers included inside the VPC are capable of effectively pinging one another via IPv6. These systems, however, are incapable of communicating with the external vendor.

What modifications are necessary to facilitate 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.

Commented [LC16]: D
NAT gateways are not supported for IPv6 traffic—use an egress-only internet gateway instead.
https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

Question #404

On AWS, a business is developing an application. For analysis, the application transmits log files to an Amazon Elasticsearch Service (Amazon ES) cluster. Each piece of data must be contained inside a VPC.
A number of the company's developers work remotely. Other developers are based at three distinct business locations. The developers must connect to Amazon ES directly from their local development computers in order to study and display logs.

Which solution will satisfy these criteria?

- A. Configure and set up an AWS Client VPN endpoint. Associate the Client VPN endpoint with a subnet in the VPC. Configure a Client VPN self-service portal. Instruct the developers to connect by using the client for Client VPN.
- B. Create a transit gateway, and connect it to the VPC. Create an AWS Site-to-Site VPN. Create an attachment to the transit gateway. Instruct the developers to connect by using an OpenVPN client.
- C. Create a transit gateway, and connect it to the VPC. Order an AWS Direct Connect connection. Set up a public VIF on the Direct Connect connection. Associate the public VIF with the transit gateway. Instruct the developers to connect to the Direct Connect connection
- D. Create and configure a bastion host in a public subnet of the VPC. Configure the bastion host security group to allow SSH access from the company CIDR ranges. Instruct the developers to connect by using SSH.

Commented [LC17]: B - It is either On prem - TGW - VPC attachment OR On prem - VPN - VPC attachment. Would not make sense to do both in this scenario. Redundancy is not the focus here. Plus OpenVPN client will be used as a client to site solution by developers. Hence this option is WRONG.
C – DirectConnect is overkill for the requirement.
D - ElasticSearch is GUI based so SSH will not help here.

Option A satisfies the criterias.

Question #405

On AWS, a business hosts a software-as-a-service (SaaS) application. The application is composed of AWS Lambda functions and a MySQL Multi-AZ database on Amazon RDS. During market events, the application's burden is significantly increased. Users have slower response times during peak hours due to the high volume of database connections. The organization needs to enhance the database's scalability and availability.

Which solution satisfies these criteria?

- A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
- B. Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function.
- C. Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records.
- D. Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

Commented [LC18]: This only solves read performance, what about DB connection issues?
Answer should be D.

Solves connection pooling and read replica. Plus, Aurora is much better in terms of performance.

Question #406

A cluster of Amazon EC2 instances has been setup as a high-performance computing (HPC) cluster using a collection of Amazon EC2 instances. The instances are operating in a placement group and are capable of communicating at up to 20 Gbps network rates.
The cluster must communicate with an EC2 instance that is not a member of the placement group. The control instance is setup with a public IP address and uses the same instance type and AMI as the other instances.

How can the Solutions Architect optimize network performance between the control instance and the placement group instances?

- A. Terminate the control instance and relaunch it in the placement group.
- B. Ensure that the instances are communicating using their private IP addresses.
- C. Ensure that the control instance is using an Elastic Network Adapter.
- D. Move the control instance inside the placement group.

Commented [LC19]: The answer is D for sure. This is out of the site docs. It ONLY needs to be stopped not terminated to be moved.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#change-instance-placement-group

Change the placement group for an instance
You can change the placement group for an instance in any of the following ways:

Move an existing instance to a placement group

Move an instance from one placement group to another

Remove an instance from a placement group

Before you move or remove the instance, the instance must be in the stopped state. You can move or remove an instance using the AWS CLI or an AWS SDK.

Question #407

A business is building a web application that will be hosted on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer (ALB).
The application is only accessible to users from a specified country. The firm need the ability to track prohibited access requests. The solution should be as low-maintenance as feasible.

Which solution satisfies these criteria?

- A. Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- C. Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.
- D. Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

Commented [LC20]: WAF is designed to serve this case, for A making a IP list is impossible. AWS has such list, and can guarantee 99.8% accurate, how can a company do it?

Question #408

An online store must process vast product catalogs on a regular basis, which are processed in batches. These are delivered to Amazon Mechanical Turk users for processing, but the company has requested its Solutions Architect to develop a workflow orchestration system that enables it to manage many concurrent Mechanical Turk operations, manage the outcome evaluation process, and reprocess failures.

Which of the following choices provides the retailer with the LEAST amount of implementation effort for interrogating the status of each workflow?

- 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.

Commented [LC21]: See use case #2 in ref.

Ref. https://aws.amazon.com/swf/faqs/?nc1=h_ls

Question #409

A corporation has an on-premises monitoring system that stores events in a PostgreSQL database. Due to high ingestion, the database is unable to scale and regularly runs out of storage.
The business is pursuing a hybrid approach and has already established a VPN link between its network and AWS. The solution must include the following characteristics:
⇨ Managed Amazon Web Services (AWS) services to reduce operational complexity.
⇨ A buffer that grows automatically in response to data traffic and needs no continuing management.
⇨ A dashboard-creation tool for monitoring events in near-real time.
⇨ Support for JSON data that is semi-structured and dynamic schemas.

Which component combination will allow the business to develop a monitoring system that satisfies these requirements? (Select two.)

- A. Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.
- B. Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events.
- C. Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.
- D. Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.
- E. Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

Commented [LC22]: Managed, auto-scales and pushes data to ES.

Commented [LC23]: Semi-structured and dynamic schema

Question #410

A business has built a web application that is hosted on Amazon EC2 instances in a single AWS Region. The firm has expanded its operations into new nations and needs to expand its application into additional locations to fulfill its consumers' low-latency requirements. The regions may be partitioned, and an application operating in one area need not interact with instances running in other regions.

How could the company's Solutions Architect automate the application's deployment so that it may be deployed MOST EFFECTIVELY across numerous regions?

- A. Write a bash script that uses the AWS CLI to query the current state in one region and output a JSON representation. Pass the JSON representation to the AWS CLI, specifying the --region parameter to deploy the application to other regions.
- B. Write a bash script that uses the AWS CLI to query the current state in one region and output an AWS CloudFormation template. Create a CloudFormation stack from the template by using the AWS CLI, specifying the --region parameter to deploy the application to other regions.
- C. Write a CloudFormation template describing the application's infrastructure in the resources section. Create a CloudFormation stack from the template by using the AWS CLI, specify multiple regions using the --regions parameter to deploy the application.
- D. Write a CloudFormation template describing the application's infrastructure in the Resources section. Use a CloudFormation stack set from an administrator account to launch stack instances that deploy the application to other regions.

Commented [LC24]: D
A stack set lets you create stacks in AWS accounts across regions by using a single AWS CloudFormation template. All the resources included in each stack are defined by the stack set's AWS CloudFormation template. As you create the stack set, you specify the template to use, as well as any parameters and capabilities that template requires.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html

Question #411

A business uses Amazon CloudFront, Amazon API Gateway, and AWS Lambda services to power a serverless application. Currently, the application code is deployed by creating a new version number for the Lambda function and updating it using an AWS CLI script. If an error occurs with the new function version, another CLI script reverts to the prior functioning version of the function. The organization wishes to lower the time required to deploy new versions of the application logic given by Lambda functions, as well as the time required to discover and reverse problems.

How is this possible?

- A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function. For changes to Lambda, create an AWS CloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
- B. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code. Rollback if Amazon CloudWatch alarms are triggered.
- C. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version.
- D. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint.

Commented [LC25]: B
https://aws.amazon.com/about-aws/whats-new/2017/11/aws-lambda-supports-traffic-shifting-and-phased-deployments-with-aws-codedeploy/

D would need too much time.

Question #412

Which of the following cannot be done after configuring 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.

Commented [LC26]: https://docs.aws.amazon.com/directconnect/latest/UserGuide/migratevirtualinterface.html

Question #413

A business is using the AWS Cloud to host a bespoke database. Amazon Elastic Computing Cloud (Amazon EC2) is used for compute while Amazon Elastic Block Store (Amazon EBS) is used for storage. The database is hosted on Amazon EC2 instances of the newest generation and data is stored on a General Purpose SSD (gp2) EBS disk.

The current volume of data is as follows:

⇨ The volume is 512 GB in size.
⇨ The volume never goes above 256 GB utilization.
⇨ The volume consistently uses around 1,500 IOPS.

A solutions architect must analyze the present database storage layer and give recommendations on cost-cutting measures.

Which method will result in the MOST cost reduction while maintaining the database's performance?

- A. Convert the data volume to the Cloud HDD (sc1) type. Leave the volume as 512 GB. Set the volume IOPS to 1,500.
- B. Convert the data volume to the Provisioned IOPS SSD (io2) type. Resize the volume to 256 GB. Set the volume IOPS to 1,500.
- C. Convert the data volume to the Provisioned IOPS SSD (io2) Block Express type. Leave the volume as 512 GB. Set the volume IOPS to 1,500.
- D. Convert the data volume to the General-Purpose SSD (gp3) type. Resize the volume to 256 GB. Set the volume IOPS to 1,500.

Commented [LC27]: Even though the minimum for gp3 is 3000 IOPS, it's still much cheaper than the io2, with the same volume size.

Question #414

A bank is migrating its mainframe-based credit card acceptance processing program to the AWS cloud.
At peak demand, the new application will get up to 1,000 requests per second. Each transaction consists of numerous stages, each of which must receive the outcome of the preceding step. The full request must return an authorized response with no data loss in less than two seconds. Each request must be addressed. Payment Card Industry Data Security Standard (PCI DSS) compliance is required.

Which solution satisfies all of the bank's goals with the LEAST amount of complexity and expense while still complying with regulatory 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.

Commented [LC28]: https://aws.amazon.com/compliance/services-in-scope/

Answer is D. The throughput of standard SQS is unlimited. Although the request processing may appear asynchronous, finishing all steps in 2 sec won't be an issue. From the perspective of setting up a solution, A might be most easy but it is not reliable. It will pose issues when operating this solution in terms of handling failures and losing data. Therefore I think D is the right answer. If a DLQ was specified as part of option A, then I would have voted for Option A. But I think the correct answer is D.

Question #415

A solutions architect must advise a business on how to transition its on-premises data processing application to Amazon Web Services (AWS). At the moment, users submit input files using a web site. The web server then uploads the files to the NAS and communicates with the processing server through a message queue. Processing each media file might take up to an hour. The organization has established that the volume of media files awaiting processing is much larger during business hours and swiftly decreases after hours.

Which migration suggestion is the MOST cost-effective?

- A. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in an Amazon S3 bucket.
- B. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files. Store the processed files in Amazon EFS. Shut down the EC2 instance after the task is complete.
- C. Create a queue using Amazon MQ. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files. Store the processed files in Amazon EFS.
- D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket.

Commented [LC29]: D. Create a queue using Amazon SQS. Configure the existing web server to publish to the new queue. Use Amazon EC2 instances in an EC2 Auto Seating group to pull requests from the queue and process the files. Scale the EC2 instances based on the SQS queue length. Store the processed files in an Amazon S3 bucket.

Lambdas are ruled out because of their timeout. MQ is ruled out.

Question #416

An IAM user is attempting to conduct an action on an item that is part of the bucket of another root account.

Which of the following will AWS S3 not verify?

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

Commented [LC30]: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-auth-workflow-bucket-operation.html

Example #4.

Question #417

Amazon Aurora MySQL is being used by a business to power a customer relationship management (CRM) application. The program needs regular database and Amazon EC2 instance maintenance. System administrators authenticate against AWS Identity and Access Management (IAM) using an internal identity provider to obtain access to the AWS Management Console. Each system administrator has a user name and password that were previously set inside the database for database access.

A recent security assessment discovered that database passwords are not changed on a regular basis. The organization wishes to replace the passwords with temporary credentials using the AWS access restrictions already in place.

Which collection of solutions best meets the needs of the business?

- A. Create a new AWS Systems Manager Parameter Store entry for each database password. Enable parameter expiration to invoke an AWS Lambda function to perform password rotation by updating the parameter value. Create an IAM policy allowing each system administrator to retrieve their current password from the Parameter Store. Use the AWS CLI to retrieve credentials when connecting to the database.
- B. Create a new AWS Secrets Manager entry for each database password. Configure password rotation for each secret using an AWS Lambda function in the same VPC as the database cluster. Create an IAM policy allowing each system administrator to retrieve their current password. Use the AWS CLI to retrieve credentials when connecting to the database.
- C. Enable IAM database authentication on the database. Attach an IAM policy to each system administrator's role to map the role to the database user name. Install the Amazon Aurora SSL certificate bundle to the system administrators' certificate trust store. Use the AWS CLI to generate an authentication token used when connecting to the database.
- D. Enable IAM database authentication on the database. Configure the database to use the IAM identity provider to map the administrator roles to the database user. Install the Amazon Aurora SSL certificate bundle to the system administrators' certificate trust store. Use the AWS CLI to generate an authentication token used when connecting to the database.

Commented [LC31]: A and B are wrong: it does not address the use of temporary credentials and using existing company controls. It will just rotate existing credentials but not use temporary ones.

C and D are in the fight... from a technical perspective D would be better BUT I could not find any doc that explains how to leverage an IdP with IAM DB Auth, so I would go for C as it follows the current process to grant an IAM user DB rights.

Question #418

A business wishes to examine log data utilizing date ranges via the use of a bespoke application hosted on AWS. Each day, the program creates around 10 GB of data, which is likely to expand. A Solutions Architect is assigned with the responsibility of storing the data in Amazon S3 and analyzing it using Amazon Athena.

Which sequence of steps will provide the best performance as the data grows? (Select 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.

Commented [LC32]:

Commented [LC33]:

Question #419

Which of the following AWS Data Pipeline components polls for and executes tasks?

- A. Pipeline Definition
- B. Task Runner
- C. Amazon Elastic MapReduce (EMR)
- D. AWS Direct Connect

Commented [LC34]: Task Runner polls for tasks and then performs those tasks.
Reference:
http://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/what-is-datapipeline.html

Question #420

AWS Organizations is being used by a business to manage several AWS accounts. For security reasons, the organization needs the development of an Amazon Simple Notification Service (Amazon SNS) topic in each Organizations member account that permits interaction with a third-party alerting system.
To automate the deployment of CloudFormation stacks, a solutions architect utilized an AWS CloudFormation template to construct the SNS topic and stack sets.
Organizations have enabled trusted access.

What should the solutions architect do to ensure that the CloudFormation StackSets are deployed across all AWS accounts?

- A. Create a stack set in the Organizations member accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.
- B. Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.
- C. Create a stack set in the Organizations master account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.
- D. Create stacks in the Organizations master account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

Commented [LC35]: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-orgs-manage-auto-deployment.html

Question #421

Currently, a web design business maintains numerous FTP servers, which are used by its 250 clients to upload and download huge graphic assets. They desire to migrate this system to AWS in order to increase its scalability, but they also wish to preserve client privacy and keep expenses low.

Which Amazon Web Services architecture would you recommend?

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

Commented [LC36]: A is correct.

Limit is 1000 buckets but still creating a bucket per user is overkill for what is needed, so B and D are ruled out.

C is too expensive and AWS allows to directly use S£ for this.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/BucketRestrictions.html

Question #422

Five IAM users have been established by an organization. The organization want to provide them with a same login ID but separate passwords.

How is the organization to do this?

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

Commented [LC37]:

Question #423

A large organization want to enable its developers to buy third-party software through AWS Marketplace. The corporation employs an AWS Organizations account structure with all capabilities enabled, and each organizational unit (OU) has a shared services account that procurement managers will use. According to the procurement team's guideline, developers should be allowed to purchase third-party software only from an authorized list and should do so via AWS Marketplace's Private Marketplace. The procurement team desires that management of Private Marketplace be limited to a job called procurement-manager-role, which procurement managers may adopt. Other IAM users, groups, roles, and account administrators within the organization should be disallowed administrative access to the Private Marketplace.

What is the MOST EFFECTIVE method for developing an architecture that satisfies these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization.

Commented [LC38]:

Question #424

A business is using the AWS Cloud to host numerous workloads. The organization has distinct software development departments. The organization leverages AWS Organizations and SAML-based federation to provide developers authority to handle resources in their AWS accounts. Each development unit deploys its production workloads to a single shared production account.
Recently, on the production account, an event happened in which members of one development unit terminated an EC2 instance that belonged to another development unit. A solutions architect must provide a solution that eliminates the possibility of a similar situation occurring in the future. Additionally, the solution must enable developers to control the instances utilized to run their workloads.

Which technique will satisfy these criteria?

- A. Create separate OUs in AWS Organizations for each development unit. Assign the created OUs to the company AWS accounts. Create separate SCPs with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU.
- B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit.
- C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit. Assign the SCP to the root OU.
- D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role.

Commented [LC39]: B is the correct answer.

A - Does not make much sense. An account can only belong to one OU. This is a single production account so it can't be in multiple OUs.
B - Session tag is used to identify which business unit a user is part of. IAM policy prevent them from modifying resources for any business unit but their own.
C. This does not restrict any existing permissions so users can still modify resources from different business units.
D. STS cannot be used to assign a policy to an IAM role. A policy has to be assigned to the role before authentication occurs.

Question #425

On AWS, a business is developing a software-as-a-service (SaaS) offering. The organization has implemented an Amazon API Gateway REST API integrated with AWS Lambda across various AWS Regions and in the same production account.
The company's pricing structure is tiered, allowing users to pay for the capability to perform a certain number of API requests each second. The premium tier enables users to make up to 3,000 calls per second and is identifiable by a unique API key. Several premium tier customers across several regions report receiving 429 Too Many Requests error answers from multiple API calls during high use hours. The Lambda function is never called, as seen by the logs.

What may be causing these customers' error messages?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

Commented [LC40]: I thought this one was tough tbh, because both Lambda concurrency issues and API gateway throttling can cause this error. My logic in the end was that it was C, because of the numbers quoted in https://docs.aws.amazon.com/apigateway/latest/developerguide/limits.html. In essence the requests per second limit per *account* is 10,000, so selling premium subscriptions that allow up to 3000 isn't scalable, and there is no mention of an account per API. Moreover, that link seems to suggest that regional APIs are 600p/s.

A, B are ruled out because the lambda is never called.

Question #426

A business intends to create a management network on the AWS VPC. The business is attempting to protect the webserver on a single VPC instance in such a way that both internet and back-end administration traffic is permitted. The business wants to configure the back-end administration network interface to accept SSH traffic exclusively from a certain IP range, but the webserver facing the internet will have an IP address that accepts traffic from all internet IPs.

How can the business do this with a single web server instance?

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

Commented [LC41]: Note: Different subnets doesn't mean different AZs.

Correct Answer C:
Scenarios for network interfaces

Attaching multiple network interfaces to an instance is useful when you want to:
Create a management network.
Use network and security appliances in your VPC.
Create dual-homed instances with workloads/roles on distinct subnets.
Create a low-budget, high-availability solution.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/scenarios-enis.html

Question #427

A huge on-premises Apache Hadoop cluster with a 20 PB HDFS database is used by a business. Each quarter, the cluster grows by around 200 instances and 1 PB. The company's objectives are to allow Hadoop data resilience, to mitigate the effect of cluster node failures, and to dramatically cut expenses. The present cluster is available 24 hours a day and is capable of handling a wide range of analytical workloads, including interactive queries and batch processing.

Which solution would match these criteria with the LEAST amount of price and downtime?

- 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.

Commented [LC42]: To migrate large datasets of 10 PB or more in a single location, you should use Snowmobile. For datasets less than 10 PB or distributed in multiple locations, you should use Snowball. In addition, you should evaluate the amount of available bandwidth in your network backbone. If you have a high speed backbone with hundreds of Gb/s of spare throughput, then you can use Snowmobile to migrate the large datasets all at once. If you have limited bandwidth on your backbone, you should consider using multiple Snowballs to migrate the data incrementally.

Question #428

A user is running a batch process on EC2 instances that are EBS-backed. The batch process starts a few Amazon EC2 instances to perform Hadoop Map reduce tasks, which may take between 50 and 600 minutes or even longer. The user desires a setting that allows the instance to be terminated only when the procedure is complete.

How does the user setup CloudWatch for this?

- 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

Commented [LC43]: 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 #429

A business created a Java application and deployed it on an Amazon EC2 instance running an Apache Tomcat server. The company's Engineering team utilized AWS CloudFormation and Chef Automate to automate the provisioning and updating of the application's infrastructure and configuration in development, test, and production environments. These implementations have resulted in a considerable increase in the dependability of change release. The Engineering team indicates that service outages occur often as a result of unanticipated issues encountered when upgrading the Apache Tomcat server's application.

Which option will make all releases more reliable?

- A. Implement a blue/green deployment methodology.
- B. Implement the canary release methodology.
- C. Configure Amazon CloudFront to serve all requests from the cache while deploying the updates.
- D. Implement the all at once deployment methodology.

Commented [LC44]: The answer is Blue/Green. The question requires a "Reliable" soluton - With Canary you would still be routing to a small subset of user base who would be impacted if there is an issue with upgrade. With Blue/Green you would test in one environment and once it works fine you could swing over - that way there will be no customer impact or production issue.

Question #430

A Solutions Architect is responsible for developing a patch management strategy for a big mixed fleet of Windows and Linux systems. The patching strategy must be executed securely, be audit-ready, and adhere to the business objectives of the organization.

Which solution satisfies these needs with the LEAST amount of effort?

- A. Install and use an OS-native patching service to manage the update frequency and release approval for all instances. Use AWS Config to verify the OS state on each instance and report on any patch compliance issues.
- B. Use AWS Systems Manager on all instances to manage patching. Test patches outside of production and then deploy during a maintenance window with the appropriate approval.
- C. Use AWS OpsWorks for Chef Automate to run a set of scripts that will iterate through all instances of a given type. Issue the appropriate OS command to get and install updates on each instance, including any required restarts during the maintenance window.
- D. Migrate all applications to AWS OpsWorks and use OpsWorks automatic patching support to keep the OS up-to-date following the initial installation. Use AWS Config to provide audit and compliance reporting.

Commented [LC45]: Patch Manager provides options to scan your instances and report compliance on a schedule, install available patches on a schedule, and patch or scan instances on demand whenever you need to. You can also generate patch compliance reports that are sent to an Amazon Simple Storage Service (Amazon S3) bucket of your choice. You can generate one-time reports, or generate reports on a regular schedule. For a single instance, reports include details of all patches for the instance. For a report on all instances, only a summary of how many patches are missing is provided.

Ref.
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html

Question #431

A client has created a connection to AWS using AWS Direct Connect. Although the connection is operational and routes are listed on the client's end, the customer is unable to connect EC2 instances inside its VPC to servers in its datacenter.

Which of the following choices represents a feasible means of resolving this situation? (Select two.)

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

Commented [LC46]: B and E correct:
https://aws.amazon.com/premiumsupport/knowledge-center/routing-dx-private-virtual-interface/

Commented [LC47]:

Question #432

A life sciences business processes genomics data using a mix of open-source tools and Docker containers running on servers in its on-premises data center. Data for sequencing is created and stored on a local storage area network (SAN), followed by processing.
The research and development teams are experiencing capacity constraints and have chosen to re-architect their genomics analysis platform on AWS to enable it to grow in response to workload needs and shorten turnaround time from weeks to days.
The business is connected to AWS through a high-speed AWS Direct Connect connection. Sequencers create around 200 GB of data for each genome, and processing the data with optimal computational capability may take several hours. The resulting file will be uploaded to Amazon S3. Each day, the organization anticipates receiving 10-15 employment applications.

Which solution satisfies these criteria?

- A. Use regularly scheduled AWS Snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use S3 events to trigger an AWS Lambda function to process the data.
- B. Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto Scaling group to launch custom-AMI EC2 instances running the Docker containers to process the data.
- C. Use AWS DataSync to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Lambda function that starts an AWS Step Functions workflow. Store the Docker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.
- D. Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS Batch job that executes on Amazon EC2 instances running the Docker containers to process the data.

Commented [LC48]: Agree on C.
For instance:
https://docs.aws.amazon.com/whitepapers/latest/genomics-data-transfer-analytics-and-machine-learning/transferring-genomics-data-to-the-cloud-and-establishing-data-access-patterns-using-aws-datasync-and-aws-storage-gateway-for-files.html => Use AWS DataSync to transfer data to Amazon S3

Question #433

A business is experiencing difficulties with its recently installed serverless infrastructure, which makes use of Amazon API Gateway, Amazon Lambda, and Amazon DynamoDB.
The application operates as anticipated in steady state. However, during periods of high stress, tens of thousands of concurrent invocations are required, and user requests often fail before succeeding. The organization examined the logs for each component, with a particular emphasis on the Amazon CloudWatch Logs for Lambda.
The services and apps have not registered any faults.

What may be causing this issue?

- 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.

Commented [LC49]: Answer is C. When throttle limits are low on API Gateway, concurrent requests beyond that threshold limit are dropped and they need to be retried. As a result, after repeated retries the request succeeds when the concurrent request count drops below the throttle limit.

Question #434

A corporation wishes to increase their Amazon EMR platform's cost awareness. The organization has budgeted for each team's use of Amazon EMR. When a budgetary threshold is crossed, an email should be sent to the budget office's distribution list notifying them. Teams should be able to check the total cost of their EMR cluster. A solutions architect must develop a system that proactively and centrally enforces the policy in a multi-account environment.

Which measures should the solutions architect do in combination to satisfy these requirements? (Select two.)

- A. Update the AWS CloudFormation template to include the AWS::Budgets::Budget::resource with the NotificationsWithSubscribers property.
- B. Implement Amazon CloudWatch dashboards for Amazon EMR usage.
- C. Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscribers actions.
- D. Create an AWS Service Catalog portfolio for each team. Add each team's Amazon EMR cluster as an AWS CloudFormation template to their Service Catalog portfolio as a Product.
- E. Create an Amazon CloudWatch metric for billing. Create a custom alert when costs exceed the budgetary threshold.

Commented [LC50]: I will go with A & D

You can use AWS Budgets to track your service costs and usage within AWS Service Catalog. You can associate budgets with AWS Service Catalog products and portfolios. AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.
If a budget is associated to a product, you can view information about the budget on the Products and Product details page. If a budget is associated to a portfolio, you can view information about the budget on the Portfolios and Portfolio details page.
When you click on a product or portfolio, you are taken to a detail page. These Portfolio detail and Product detail pages have a section with detailed information about the associated budget. You can see the budgeted amount, current spend, and forecasted spend. You also have the option to view budget details and edit the budget.

Commented [LC51]:

Question #435

An education corporation manages an online program that is utilized by college students worldwide. The application is hosted in an Amazon Elastic Container Service (Amazon ECS) cluster behind an Application Load Balancer (ALB). A system administrator notices a weekly increase in the number of unsuccessful login attempts, which overwhelms the authentication service for the application. All unsuccessful login attempts come from around 500 unique IP addresses that vary on a weekly basis. A solutions architect must ensure that the authentication service is not overwhelmed by unsuccessful login attempts.

Which option satisfies these conditions the most efficiently?

- A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses
- B. Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Block. Connect the web ACL to the ALB
- C. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges
- D. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block. Conne ct the web ACL to the ALB

Commented [LC52]: Going with B.
Rate-base rule in the WAF
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html

Question #436

A business runs an application on an Amazon EC2 instance and requires file storage in Amazon S3. The data should never be sent over the public internet, and access to a particular Amazon S3 bucket should be restricted to the application's EC2 instances. A solutions architect has constructed an Amazon S3 VPC endpoint and linked it to the application's VPC.

What further efforts should the solutions architect take to ensure compliance with these requirements?

- A. Assign an endpoint policy to the endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint. Add the gateway prefix list to a NACL of the instances to limit access to the application EC2 instances only.
- B. Attach a bucket policy to the S3 bucket that grants access to application EC2 instances only using the aws:SourceIp condition. Update the VPC route table so only the application EC2 instances can access the VPC endpoint.
- C. Assign an endpoint policy to the VPC endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint. Assign an IAM role to the application EC2 instances and only allow access to this role in the S3 bucket's policy.
- D. Assign an endpoint policy to the VPC endpoint that restricts access to S3 in the current Region. Attach a bucket policy to the S3 bucket that grants access to the VPC private subnets only. Add the gateway prefix list to a NACL to limit access to the application EC2 instances only.

Commented [LC53]: My Answer is C. In order to make VPC endpoint work, needs to add a ACL for endpoint

A: it shoud add a route for VPC endpoint, not add a NACL.

B: aws:SourceIp doesn't work, use aws:SourceVpc or aws:SourceVpce.

D: same as A.

Question #437

On AWS, a business wants to operate a serverless application. The firm intends to deploy its application using Docker containers on an Amazon ECS cluster.
A MySQL database is required for the application, and the firm intends to utilize Amazon RDS. The firm contains records that must be viewed regularly for the first three months and then very seldom afterwards. The document must be kept for a period of seven years.

Which approach is the MOST cost-effective in meeting these requirements?

- A. Create an ECS cluster using On-Demand Instances. Provision the database and its read replicas in Amazon RDS using Spot Instances. Store the documents in an encrypted EBS volume, and create a cron job to delete the documents after 7 years.
- B. Create an ECS cluster using a fleet of Spot Instances, with Spot Instance draining enabled. Provision the database and its read replicas in Amazon RDS using Reserved Instances. Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier, then delete the documents from Amazon S3 Glacier that are more than 7 years old.
- C. Create an ECS cluster using On-Demand Instances. Provision the database and its read replicas in Amazon RDS using On-Demand Instances. Store the documents in Amazon EFS. Create a cron job to move the documents that are older than 3 months to Amazon S3 Glacier. Create an AWS Lambda function to delete the documents in S3 Glacier that are older than 7 years.
- D. Create an ECS cluster using a fleet of Spot Instances with Spot Instance draining enabled. Provision the database and its read replicas in Amazon RDS using On-Demand Instances. Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier, then delete the documents in Amazon S3 Glacier after 7 years.

Commented [LC54]: A with RDS on spot instances is automatically ruled out
B is feasible by using a "Diversified" allocation strategy when setting up the Spot provisioning ECS cluster
C is feasible but more expensive to do RDS on-demand instances than RDS RI as in B, and uses EFS instead of S3 to store the documents, not as cost effective
D is feasible but more expensive to do RDS on-demand instances than RDS RI as in B

https://aws.amazon.com/ec2/spot/containers-for-less/get-started/
https://aws.amazon.com/ec2/spot/instance-advisor/

Question #438

A business maintains many apps in an on-premises data center. The data center hosts a mixture of Windows and Linux virtual machines that are controlled by VMware vCenter.
A solutions architect must develop a strategy for migrating apps to AWS. The solutions architect, however, realizes that the application's documentation is out of date and that there are no full infrastructure diagrams. The company's developers are unable to meet with the solutions architect to discuss their apps and current use.

What should the solutions architect do to assemble the necessary data?

- A. Deploy the AWS Server Migration Service (AWS SMS) connector using the OVA image on the VMware cluster to collect configuration and utilization data from the VMs.
- B. Use the AWS Migration Portfolio Assessment (MPA) tool to connect to each of the VMs to collect the configuration and utilization data.
- C. Install the AWS Application Discovery Service on each of the VMs to collect the configuration and utilization data.
- D. Register the on-premises VMs with the AWS Migration Hub to collect configuration and utilization data.

Commented [LC55]: Ans: C
Reason: AWS Application Discovery Service collects and presents configuration, usage, and behavior data from your servers to help you better understand your workloads.
Link: https://aws.amazon.com/application-discovery/

A is wrong because its use is to migrate.

Question #439

Amazon EC2 acts as a repository for public data sets that may be linked smoothly into AWS cloud-based applications.

How much does it cost to use public data sets on a monthly basis?

- 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

Commented [LC56]: https://aws.amazon.com/about-aws/whats-new/2008/12/03/public-data-sets-on-aws-now-available/

https://aws.amazon.com/opendata/open-data-sponsorship-program/

Question #440

The site reliability engineer for a corporation is doing an evaluation of Amazon FSx for Windows File Server installations inside a newly acquired account. All Amazon FSx file systems must be designed to be highly available across Availability Zones, according to company policy.

The site reliability engineer learns during the evaluation that one of the Amazon FSx file systems was deployed using the Single-AZ 2 deployment type. A solutions architect must reduce downtime while adhering to business policies about this Amazon FSx file system.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Reconfigure the deployment type to Multi-AZ for this Amazon FSx file system.
- B. Create a new Amazon FSx file system with a deployment type of Multi-AZ. Use AWS DataSync to transfer data to the new Amazon FSx file system. Point users to the new location.
- C. Create a second Amazon FSx file system with a deployment type of Single-AZ 2. Use AWS DataSync to keep the data in sync. Switch users to the second Amazon FSx file system in the event of failure.
- D. Use the AWS Management Console to take a backup of the Amazon FSx file system. Create a new Amazon FSx file system with a deployment type of Multi- AZ. Restore the backup to the new Amazon FSx file system Point users to the new location.

Commented [LC57]: B should be right answer - refer FAQ for usage of Data Sync.
If you'd like to migrate your existing files to Amazon FSx for Windows File Server file systems, we recommend the use of AWS DataSync, an online data transfer service designed to simplify, automate, and accelerate copying large amounts of data to and from AWS storage services.

Question #441

A large-scale migration to AWS was just completed by a corporation. Development teams that service many business units each have their own AWS Organizations account. A central cloud team is in charge of determining which services and resources may be used, as well as developing operational plans for all corporate teams. Certain teams are nearing the end of their account service limits. The cloud team must develop an automated and operationally efficient system for monitoring service quotas in real time. Monitoring should occur every 15 minutes and trigger alarms when a team's usage surpasses 80%.

Which solution will satisfy these criteria?

- A. Create a scheduled AWS Config rule to trigger an AWS Lambda function to call the GetServiceQuota API. If any service utilization is above 80%, publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert the cloud team. Create an AWS CloudFormation template and deploy the necessary resources to each account.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that triggers an AWS Lambda function to refresh the AWS Trusted Advisor service limits checks and retrieve the most current utilization and service limit data. If the current utilization is above 80%, publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert the cloud team. Create AWS CloudFormation StackSets that deploy the necessary resources to all Organizations accounts.
- C. Create an Amazon CloudWatch alarm that triggers an AWS Lambda function to call the Amazon CloudWatch GetInsightRuleReport API to retrieve the most current utilization and service limit data. If the current utilization is above 80%, publish an Amazon Simple Email Service (Amazon SES) notification to alert the cloud team. Create AWS CloudFormation StackSets that deploy the necessary resources to all Organizations accounts.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that triggers an AWS Lambda function to refresh the AWS Trusted Advisor service limits checks and retrieve the most current utilization and service limit data. If the current utilization is above 80%, use Amazon Pinpoint to send an alert to the cloud team. Create an AWS CloudFormation template and deploy the necessary resources to each account.

Commented [LC58]: B is correct.
A: Lambda should be invoked by cloudwatch on a schedule, not by Config.
C & D: does not make much sense to me.

Question #442

You're developing a personal document archiving system for your multinational corporation, which employs thousands of people. Each employee's data is potentially several gigabytes in size and must be backed up using this archiving system. Employees will be able to access the solution through an application, which will allow them to simply drag and drop their files into the archiving system. Employees may access their archives using a web-based interface. The corporate network is connected to AWS through a high-bandwidth AWS Direct Connect connection. You are required by law to encrypt all data before to uploading it to the cloud.

How can you achieve this in a manner that is both highly accessible and cost-effective?

- 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 serve r with sufficient storage to temporarily store, encrypt, and upload files directly into Amazon Glacier.
- C. Manage encryption keys in Amazon Key Management Service (KMS), upload to Amazon Simple Storage Service (S3) with client-side encryption using a KMS customer master key ID, and configure Amazon S3 lifecycle policies to 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.

Commented [LC59]: You can use the Amazon S3 Encryption Client in the AWS SDK in your own application to encrypt objects and upload them to Amazon S3. This method allows you to encrypt your data locally to ensure its security as it passes to the Amazon S3 service. The Amazon S3 service receives your encrypted data; it does not play a role in encrypting or decrypting it.

The Amazon S3 Encryption Client encrypts the object by using envelope encryption. The client calls AWS KMS as a part of the encryption call you make when you pass your data to the client. AWS KMS verifies that you are authorized to use the customer master key (CMK) that you specify and, if so, returns a new plaintext data key and the data key encrypted under the CMK. The Amazon S3 Encryption Client encrypts the data by using the plaintext key and then deletes the key from memory. The encrypted data key is sent to Amazon S3 to store alongside your encrypted data.

References:
https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

Question #443

All data uploaded to an Amazon S3 bucket must be encrypted according to the company's security policy. The encryption keys must be highly accessible, and the organization must be able to regulate access on a per-user basis, with each user having access to a unique encryption key.

Which of the following architectures satisfies these criteria? (Select 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.

Commented [LC60]: My preference "B" & "D".
A: customer can not control the keys!
B: AWS-KMS managed keys, allow the user to create Master keys, and control them. It is high available as it is a managed service by AWS.
C: CloudHSM can be high available by including a second instance in different AZ.
D: Meet the requirement of management and high availability.
E: Managing the keys by CloudHSM client, not IAM user!!

Commented [LC61]:

Question #444

Amazon Elastic File System (EFS) offers information about the amount of space utilized by an item by using the network file system's space used property. The property specifies the current metered data size of the item, not the metadata size.

Which of the following tools will you use to determine how much disk space a file consumes?

- A. blkid utility
- B. du utility
- C. sfdisk utility
- D. pydf utility

Commented [LC62]: Amazon EFS reports file system sizes and sizes of objects within a file system. Using the NFSv4.1 space _ used attribute for measuring the space used for an object, it reports only the object's current metered data size and not the metadata size. There are two utilities available for measuring disk usage of a file, the du and stat utilities.
Reference:
https://docs.aws.amazon.com/efs/latest/ug/metered-sizes.html

Question #445

A significant European corporation intends to move its apps to the AWS Cloud. The corporation has many AWS accounts for different business units. According to a data privacy rule, the corporation is required to limit developers' access to AWS European Regions exclusively.

What should the solution architect do in order to satisfy this demand with the LEAST amount of administrative overhead possible?

- A. Create IAM users and IAM groups in each account. Create IAM policies to limit access to non-European Regions. Attach the IAM policies to the IAM groups.
- B. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions. Create SCPs to limit access to non-European Regions and attach the policies to the OUs.
- C. Set up AWS Single Sign-On and attach AWS accounts. Create permission sets with policies to restrict access to non-European Regions. Create IAM users and IAM groups in each account.
- D. Enable AWS Organizations, attach the AWS accounts, and create OUs for European Regions and non-European Regions. Create permission sets with policies to restrict access to non-European Regions. Create IAM users and IAM groups in the primary account.

Commented [LC63]:

Question #446

AWS client has an on-premises web application. The web application retrieves data from a firewall-protected third-party API. In each client's allow list, the third party accepts just one public CIDR block.
The client want to transfer their web application to Amazon Web Services (AWS). The application will be hosted on a collection of Amazon EC2 instances in a Virtual Private Cloud (VPC) behind an Application Load Balancer (ALB). The ALB is distributed among public subnets. Private subnets are used to host the EC2 instances. NAT gateways connect private subnets to the internet.

How can a solutions architect guarantee that the web application can continue to make calls to the third-party API after the migration?

- A. Associate a block of customer-owned public IP addresses to the VPC. Enable public IP addressing for public subnets in the VPC.
- B. Register a block of customer-owned public IP addresses in the AWS account. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC.
- C. Create Elastic IP addresses from the block of customer-owned IP addresses. Assign the static Elastic IP addresses to the ALB.
- D. Register a block of customer-owned public IP addresses in the AWS account. Set up AWS Global Accelerator to use Elastic IP addresses from the address block. Set the ALB as the accelerator endpoint.

Commented [LC64]: https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-bring-your-own-ip-byoip-for-amazon-vpc/

Question #447

A startup is nearing completion of the architecture for its backup solution for AWS apps. All apps are hosted on AWS and each tier utilizes at least two Availability Zones.
IT is required by company policy to maintain nightly backups of all data in at least two locations: production and disaster recovery. The places must be geographically distinct. Additionally, the firm requires that the backup be instantly accessible for restoration at the production data center and within 24 hours at the disaster recovery site. Ideally, all backup operations should be completely automated.

Which backup system is the MOST cost-effective and meets 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.

Commented [LC65]: D
A: Not sustainable. EBS has a 16TiB limit.
B: No backup at the production region.
C: Glacier does not allow restore immediately.

Question #448

A business is operating a distributed application on an Auto Scaling group of Amazon EC2 machines. The program saves massive volumes of data on an Amazon Elastic File System (Amazon EFS) file system and generates fresh data on a monthly basis. The organization needs to back up its data in a secondary AWS Region to use as a fallback in the event of a main Region performance issue. The company's RTO is one hour. A solutions architect must develop a backup plan while keeping the additional expense to a minimum.

Which backup method, if any, should the solutions architect propose in order to satisfy these requirements?

- A. Create a pipeline in AWS Data Pipeline. Copy the data to an EFS file system in the secondary Region. Create a lifecycle policy to move files to the EFS One Zone-Infrequent Access storage class.
- B. Set up automatic backups by using AWS Backup. Create a copy rule to copy backups to an Amazon S3 bucket in the secondary Region. Create a lifecycle policy to move backups to the S3 Glacier storage class.
- C. Set up AWS DataSync and continuously copy the files to an Amazon S3 bucket in the secondary Region. Create a lifecycle policy to move files to the S3 Glacier Deep Archive storage class.
- D. Turn on EFS Cross-Region Replication and set the secondary Region as the target. Create a lifecycle policy to move files to the EFS Infrequent Access storage class in the secondary Region.

Commented [LC66]: A - Correct
B - Cannot be restored with an RTO of 1 hour
C - Cannot be restored with an RTO of 1 hour
D - Cross-Region replication is a S3 concept. Not valid for EFS.

Note. For B and C, Expedited Retrieval is still not ideal for "fallback" reasons, but only for backup reason. You can't do failover to Glacier.

Question #449

You're successfully operating a multitier web application on AWS, and your marketing department has requested that you add a reporting tier to the service. Every 30 minutes, the reporting layer will collect and publish status reports based on user-generated data contained in your web application's database.
For the database layer, you are presently operating a Multi-AZ RDS MySQL server. Additionally, you've used Elasticache to provide a database caching layer between the application and database tiers.

Please choose the response that will enable you to properly install the reporting layer while having the least impact on your database as feasible.

- 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.

Commented [LC67]: C is correct because Cache won't represent full DB. Here, we need aggregation on whole DB which can be with Read Replica

Question #450

Your application specializes in data transformation. Transformable files are uploaded to Amazon S3 and subsequently transformed by a fleet of spot EC2 instances. Files provided by your premium clients must be processed immediately.

How should such a system be implemented?

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

Commented [LC68]:

Question #451

After establishing an instance on a public subnet to act as a NAT (Network Address Translation) device, you adjust your route tables to make the NAT device the target of your private subnet's internet-bound traffic. When attempting to establish an outbound connection to the internet from a private subnet instance, you are unsuccessful.

Which of the following approaches would be most effective in resolving 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

Commented [LC69]: Disable source/destination checks
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.
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html

Question #452

Which of the following commands takes arguments in the form of binary data?

- A. --user-data
- B. --cipher text-key
- C. --aws-customer-key
- D. --describe-instances-user

Commented [LC70]: 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.
Reference:

https://docs.aws.amazon.com/cli/latest/userguide/cli-usage-parameters-file.html#cli-usage-parameters-file-binary

Question #453

The data center of a business is linked to the AWS Cloud through a low-latency 10 Gbps AWS Direct Connect connection that includes a private virtual interface to the virtual private cloud (VPC). The firm's internet connection is 200 Mbps, and each Friday, the company creates a 150 TB dataset. On Monday morning, the data must be moved and made accessible on Amazon S3.

Which is the LEAST EXPENSIVE method of meeting the criteria while yet allowing for growth in data transfer?

- A. Order two 80 TB AWS Snowball appliances. Offload the data to the appliances and ship them to AWS. AWS will copy the data from the Snowball appliances to Amazon S3.
- B. Create a VPC endpoint for Amazon S3. Copy the data to Amazon S3 by using the VPC endpoint, forcing the transfer to use the Direct Connect connection.
- C. Create a VPC endpoint for Amazon S3. Set up a reverse proxy farm behind a Classic Load Balancer in the VPC. Copy the data to Amazon S3 using the proxy.
- D. Create a public virtual interface on a Direct Connect connection, and copy the data to Amazon S3 over the connection.

Commented [LC71]: A is not practical as Snow Ball takes more than 1 week.
B is not valid because Direct Connect can't access VPC Endpoint.
C and D are ok but C is not cost effective because you have to setup a proxy farm.

D should be correct

Question #454

If you wish to map an Amazon Elastic Block Store to an Amazon EC2 instance _____ using CloudFormation...

- A. you reference the logical IDs to associate the block stores with the instance
- B. you reference the physical IDs of the instance along with the resource type
- C. you reference the instance IDs of the block store along with the resource properties
- D. you reference the physical IDs of both the block stores and the instance

Commented [LC72]: In AWS CloudFormation, if you want to map an Amazon Elastic Block Store to an Amazon EC2 instance, you reference the logical IDs to associate the block stores with the instance.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/concept-resources.html

Question #455

A business is developing an account strategy in order to begin using AWS. The security team will provide each team the permissions necessary to adhere to the least privileged access concept. Teams want to keep their resources distinct from those of other groups, while the Finance team wants to charge separately for each team's resource utilization.

Which account creation method satisfies these criteria and allows for modifications?

- 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.

Commented [LC73]:

Question #456

When working with Numeric Conditions in IAM, it is possible to utilize condensed versions of the available comparators rather than the more verbose ones.

Which of the following is the abbreviation for the "NumericLessThanEquals" Numeric Condition?

- A. numlteq
- B. numlteql
- C. numltequals
- D. numeql

Commented [LC74]: 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. Reference: http://awsdocs.s3.amazonaws.com/SQS/2011-10-01/sqs-dg-2011-10-01.pdf

Question #457

A Solutions Architect is developing a solution for a cluster of Amazon EC2 instances that is extremely available and dependable.
The Solutions Architect is responsible for ensuring that each EC2 instance inside the cluster immediately recovers after a system failure. The solution must guarantee that the restored instance retains its original IP address.

How are these stipulations to 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.

Commented [LC75]: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

Question #458

A healthcare organization use AWS to host a production workload that holds extremely sensitive personal information. The security team has mandated that each AWS API activity performed with the root user credentials of an AWS account must immediately issue a high-priority ticket in the company's ticketing system for auditing reasons. The ticketing system includes a monthly maintenance window of three hours during which no tickets may be generated.
To comply with security standards, the organization activated AWS CloudTrail logs and created a scheduled AWS Lambda function that queries API operations done by the root user using Amazon Athena. The Lambda function notifies the ticketing system API of any activities discovered. Several tickets were not generated during a recent security assessment owing to the ticketing system being unavailable due to scheduled maintenance.

Which combination of measures should a solutions architect take to guarantee that problems are notified to the ticketing system even while scheduled maintenance is being performed?
(Select two.)

- A. Create an Amazon SNS topic to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to invoke the Lambda function.
- B. Create an Amazon SQS queue to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to publish to the SQS queue.
- C. Modify the Lambda function to be triggered by messages published to an Amazon SNS topic. Update the existing application code to retry every 5 minutes if the ticketing system's API endpoint is unavailable.
- D. Modify the Lambda function to be triggered when there are messages in the Amazon SQS queue and to return successfully when the ticketing system API has processed the request.
- E. Create an Amazon EventBridge rule that triggers on all API events where the invoking user identity is root. Configure the EventBridge rule to write the event to an Amazon SQS queue.

Commented [LC76]: The existing system can be modified to use Amazon EventBridge instead of using AWS CloudTrail with Amazon Athena. Eventbridge can be configured with a rule that checks all AWS API calls via CloudTrail. The rule can be configured to look for the usage or the root user account. Eventbridge can then be configured with an Amazon SQS queue as a target that puts a message in the queue waiting to be processed.
The Lambda function can then be configured to poll the queue for messages (event-source mapping), process the event synchronously and only return a successful result when the ticketing system has processed the request. The message will be deleted only if the result is successful, allowing for retries.
This system will ensure that the important events are not missed when the ticketing system is unavailable.

Commented [LC77]:

Question #459

Your firm maintains an on-premises multi-tier PHP online application that recently suffered outage as a result of a huge spike in web traffic after a corporate announcement. You anticipate similar announcements driving similar unanticipated bursts in the future days and are searching for strategies to swiftly boost your infrastructure's capacity to manage unexpected surges in traffic.
Currently, the application is divided into two tiers: a web tier comprised of a load balancer and many Linux Apache web servers, and a database layer comprised of a Linux server hosting a MySQL database.

Which of the following scenarios will give complete site functionality while also assisting in the enhancement of your application's capability in the short period 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.

Commented [LC78]: Answer is C
A: This works if the website is static but we don't know enough about it to determine if S3 can host it
B: is costlier and time consuming, but feasible.
C: CloudFront works with custom origins, in this case the external PHP web app. CloudFront is a good choice for handling the traffic spike in a short time
D: The scenario does not say the on-prem app is in a VM, this is not an option

Question #460

You are the administrator of a news website that updates every 15 minutes in the eu-west-1 area. The website is accessible to a global audience. It makes use of an Auto Scaling group and an Elastic Load Balancer in conjunction with an Amazon RDS database. Amazon S3 is used to store static material, which is delivered through Amazon CloudFront. Your Auto Scaling group is configured to initiate a scale up event when CPU usage reaches 60%. You're using an Amazon RDS extra large database instance with 10.000 Provisioned IOPS, a CPU usage of roughly 80%, and free RAM in the region of 2 GB.
Web analytics records indicate that the average load time for your web pages is between 1.5 and 2 seconds, while your SEO consultant desires a load time of less than 0.5 seconds.

How might you improve your visitors' website load times? (Select 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.

Commented [LC79]: Caching the DB helps with frequent queries as well as improving the instance size of RDS.

Commented [LC80]:

Commented [LC81]:

Question #461

In the United States of America, a company develops software for the CIA. The CIA agreed to host the application on Amazon Web Services (AWS), but in a secure environment. The firm is considering hosting the application on the Amazon Web Services (AWS) GovCloud region.

Which of the following statements is incorrect when an enterprise hosts on AWS GovCloud rather than the AWS standard region?

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

Commented [LC82]: AWS GovCloud (US) is an isolated AWS region designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) Region adheres to the U.S. International Traffic in Arms Regulations (ITAR) requirements. It has added advantages, such as:
Restricting physical and logical administrative access to U.S. persons only There will be a separate AWS GovCloud (US) credentials, such as access key and secret access key than the standard AWS account
The user signs in with the IAM user name and password
The AWS GovCloud (US) Region authentication is completely isolated from Amazon.com If the organization is planning to host on EC2 in AWS GovCloud then it will be billed to standard AWS account of organization since AWS GovCloud billing is linked with the standard AWS account and is not be billed separately.
Reference:
http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/whatis.html

Question #462

A business has launched a web service in two AWS Regions: us-west-2 and us-west-1. Each AWS region hosts a single instance of the web service.
Amazon Route 53 is used to direct clients to the least-latency AWS Region.
The organization want to increase the web service's availability in the event of an outage in one of the two AWS Regions.
A Solutions Architect has advised that a health check of Route 53 be conducted. The health check must identify a certain piece of text on an endpoint.

Which requirements must the endpoint satisfy in order to pass the Route 53 health check? (Select two.)

- A. The endpoint must establish a TCP connection within 10 seconds.
- B. The endpoint must return an HTTP 200 status code.
- C. The endpoint must return an HTTP 2xx or 3xx status code.
- D. The specific text string must appear within the first 5,120 bytes of the response.
- E. The endpoint must respond to the request within the number of seconds specified when creating the health check.

Commented [LC83]: CD
HTTP and HTTPS health checks – Route 53 must be able to establish a TCP connection with the endpoint within four seconds. In addition, the endpoint must respond with an HTTP status code of 2xx or 3xx within two seconds after connecting. After a Route 53 health checker receives the HTTP status code, it must receive the response body from the endpoint within the next two seconds. Route 53 searches the response body for a string that you specify. The string must appear entirely in the first 5,120 bytes of the response body or the endpoint fails the health check

Commented [LC84]:

Question #463

A corporation with worldwide offices connects to a single AWS Region using a single 1 Gbps AWS Direct Connect connection. The link is used by the company's on-premises network to interact with its AWS Cloud services. The connection is made up of a single private virtual interface that connects to a single virtual private cloud (VPC).
A solutions architect must build a solution that allows for the addition of a redundant Direct Connect connection within the same Region. Additionally, the solution must allow access to other Regions using the same pair of Direct Connect connections when the business develops into additional Regions.

Which solution satisfies these criteria?

- A. Provision a Direct Connect gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.
- B. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- C. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection and connect the new public virtual interface to the single VPC.
- D. Provision a transit gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC.

Commented [LC85]: A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.

https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

The scenario omits the fact that you will need a vgw (virtual private gateway) in all options. So, I am presuming it is safe to assume that it is present and unmentioned

Question #464 (EXAM)

A business delivers a centralized Amazon EC2 application that is housed in a single shared virtual private cloud (VPC). The centralized application must be available to client apps operating in various business units' virtual private clouds (VPCs). For scalability, the centralized application front end is equipped using a Network Load Balancer (NLB).
Up to ten virtual private clouds (VPCs) per business unit must be linked to the common VPC. Certain CIDR blocks in the business unit VPC overlap with those in the shared VPC, while others overlap with one another. Network connection to the shared VPC's centralized application should be restricted to approved business unit VPCs.

Which network configuration should a solutions architect use to link client applications in business unit virtual private clouds to the centralized application on the shared virtual private cloud?

- A. Create an AWS Transit Gateway. Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway
- B. Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service. Accept authorized endpoint requests from the endpoint service console.
- C. Create a VPC peering connection from each business unit VPC to the shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection.
- D. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs. Establish a Site-to-Site VPN connection from the business unit VPCs to the shared VPC. Configure VPC routing tables to send traffic to the VPN connection.

Commented [LC86]: A, C are ruled out because they do not allow overlapping CIDR.

NLBs always SNAT the client source IP address to their own IP within your VPC when the incoming request to the NLB via a gateway load balancer endpoint or vpc endpoint (private link):

https://docs.aws.amazon.com/vpc/latest/privatelink/endpoint-service-overview.html

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#client-ip-preservation

(This can be annoying if you want the NLB's client IP preservation feature!)

Question #465

You're a new information technology architect for a firm that sells a mobile sleep monitoring application.
When active at night, the mobile app sends 1 kilobyte of gathered data to your backend every 5 minutes.
The backend handles user authentication and data storage in an Amazon DynamoDB database.
Each morning, you scan the table to extract and aggregate data from the previous night per user, and then save the findings on Amazon S3.
Users are alerted by Amazon SNS mobile push notifications when new data becomes available, which the mobile app parses and visualizes.
Currently, you have roughly 100,000 users, the majority of them are situated in North America.
You have been entrusted with optimizing the backend system's design in order to save costs.

What would you suggest? (Select 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.

Commented [LC87]: D is wrong because there's no reason to cache if the day after data are on s3 and can be deleted.

C and E makes sense.

Commented [LC88]:

Question #466

A Solutions Architect is tasked with the responsibility of developing a deployment plan for an application layer. The following criteria apply:
⇨ Before the application code can be started, a 500 GB static dataset must be provided.
⇨ The application layer must be scalable up and down in response to demand with the least amount of starting time feasible.
⇨ Each day, the development team should be able to change the code many times.
⇨ Patches for critical operating systems (OS) must be applied within 48 hours of their release.

Which deployment approach satisfies these criteria?

- A. Use AWS Systems Manager to create a new AMI with the updated OS patches. Update the Auto Scaling group to use the patched AMI and replace existing unpatched instances. Use AWS CodeDeploy to push the application code to the instances. Store the static data in Amazon EFS.
- B. Use AWS Systems Manager to create a new AMI with updated OS patches. Update the Auto Scaling group to use the patched AMI and replace existing unpatched instances. Update the OS patches and the application code as batch job every night. Store the static data in Amazon EFS.
- C. Use an Amazon-provided AMI for the OS. Configure an Auto Scaling group set to a static instance count. Configure an Amazon EC2 user data script to download the data from Amazon S3. Install OS patches with AWS Systems Manager when they are released. Use AWS CodeDeploy to push the application code to the instances.
- D. Use an Amazon-provided AMI for the OS. Configure an Auto Scaling group. Configure an Amazon EC2 user data script to download the data from Amazon S3. Replace existing instances after each updated Amazon-provided AMI release. Use AWS CodeDeploy to push the application code to the instances.

Commented [LC89]: A. Systems Manager to update the ASG with patched AMI, CodeDeploy to push the code, and EFS for the 500 GB static data.

Question #467

A business must migrate its on-premises resources to AWS. Currently, the environment comprises of 100 virtual machines (VMs) with a combined storage capacity of 40 TB.
While the majority of VMs may be taken down since they are only used during business hours, others are mission important, and downtime must be minimized.
The on-premises network administrator allocated 10 Mbps of internet bandwidth for the move. The capacity of the on-premises network has been reached, and increasing it would be prohibitively expensive. A solutions architect must develop a migration strategy that can be implemented in the next three months.

Which approach would meet these criteria?

- A. Set up a 1 Gbps AWS Direct Connect connection. Then, provision a private virtual interface, and use AWS Server Migration Service (SMS) to migrate the VMs into Amazon EC2.
- B. Use AWS Application Discovery Service to assess each application, and determine how to refactor and optimize each using AWS services or AWS Marketplace solutions.
- C. Export the VMs locally, beginning with the most mission-critical servers first. Use AWS Transfer for SFTP to securely upload each VM to Amazon S3 after they are exported. Use VM Import/Export to import the VMs into Amazon EC2.
- D. Migrate mission-critical VMs with AWS SMS. Export the other VMs locally and transfer them to Amazon S3 using AWS Snowball. Use VM Import/Export to import the VMs into Amazon EC2.

Commented [LC90]: To transfer 40TB of data in 10Mbps link, it will take 400 days. So transferring anything over that link in 3 months is not feasible. Rules C out.

Direct Connect link is needed only while migration period. So ordering that for just 3 months doesn't seem correct. Also it's a costly option. Rules out A.

And refactoring 100 applications in 3 months, doesn't sound right to me as well. Rules out B.

So left will be D. Problem with D is that Snowball transfer also takes some time, but I guess it's OK for non critical systems to be down for week. If we can use the on-prem servers while setupping AWS instances and then transfer only the delta of data, the downtime then will be minimized.

Question #468

You've established an Auto Scaling group. The Auto Scaling group has a seven-minute cool-down time. The Auto Scaling group's initial scaling activity request is to deploy two instances. It gets the activity query at time t and launches the first instance at t+3 minutes, followed by the second instance at t+4 minutes.

After time "t," how many minutes will Auto Scaling accept another scaling activity request?

- A. 11 minutes
- B. 10 minutes
- C. 7 minutes
- D. 14 minutes

Commented [LC91]: 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.

Question #469

Is it true that Autoscaling automatically tags resources?

- A. No, not unless they are configured via API.
- B. Yes, it does.
- C. Yes, by default.
- D. No, it does not.

Commented [LC92]: 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.

Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Using_Tags.html

Question #470

A business is considering migrating an existing high-performance computing (HPC) solution to the Amazon Web Services (AWS) Cloud. The present solution is a 12-node Linux cluster with high-speed interconnection that was constructed in a single rack. A solutions architect must maximize the HPC cluster's performance.

Which combination of actions will satisfy these criteria? (Select two.)

- A. Deploy instances across at least three Availability Zones.
- B. Deploy Amazon EC2 instances in a placement group.
- C. Use Amazon EC2 instances that support Elastic Fabric Adapter (EFA).
- D. Use Amazon EC2 instances that support burstable performance.
- E. Enable CPU hyperthreading.

Commented [LC93]: A: HA is not the case
B: placement group is good for HPC, refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
C: EFA is good for HPC, refer to https://aws.amazon.com/hpc/efa/
D: burstable is not the case
E: we need to Disable hyper-threading, refer to https://www.iucc.ac.il/en/blog/best-practices-for-running-hpc-on-aws/

Commented [LC94]:

Question #471

An ecommerce business wishes to shift its order processing application to AWS. The application's data volume patterns are erratic, yet it must be available at all times. Orders must be handled on a first-come, first-serve basis and in the order in which they are received.

Which sequence of procedures should a solutions architect follow in order to satisfy these requirements?

- A. Use AWS Transfer for SFTP and upload orders as they occur. Use On-Demand Instances in multiple Availability Zones for processing.
- B. Use Amazon SNS with FIFO and send orders as they occur. Use a single large Reserved Instance for processing.
- C. Use Amazon SQS with FIFO and send orders as they occur. Use Reserved Instances in multiple Availability Zones for processing.
- D. Use Amazon SQS with FIFO and send orders as they occur. Use Spot Instances in multiple Availability Zones for processing.

Commented [LC95]: Agree, C is the best answer given

Better approach might be to:
- start with On-Demand instances in an ASG
- set the ASG scaling metric to SQS FIFO queue depth
- monitor for steady-state minimum number of instances needed
- purchase RIs for minimum number of instances needed
- use On-Demand instances for additional bursting instances in the ASG above base

Question #472

A business has a single AWS account for its environment. A solutions architect is assessing the environment and making recommendations on how the organization may enhance access to the AWS Management Console. Currently, the company's IT support staff logs into the console to do administrative duties, authenticating with named IAM users that have been assigned to their job position.

IT support personnel no longer want to manage their Active Directory and IAM user accounts concurrently. They need access to the console through their current Active Directory credentials. The solutions architect is implementing this capability using AWS Single Sign-On (AWS SSO).

Which approach will be the most cost-effective in meeting these requirements?

- A. Create an organization in AWS Organizations. Turn on the AWS SSO feature in Organizations. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure AWS SSO and set the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- B. Create an organization in AWS Organizations. Turn on the AWS SSO feature in Organizations. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure AWS SSO and select the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.
- C. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure a directory in AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) with a two-way trust to the company's on-premises Active Directory. Configure AWS SSO and select the AWS Managed Microsoft AD directory as the identity source. Create permission sets and map them to the existing groups within the AWS Managed Microsoft AD directory.
- D. Create an organization in AWS Organizations. Turn on all features for the organization. Create and configure an AD Connector to connect to the company's on-premises Active Directory. Configure AWS SSO and select the AD Connector as the identity source. Create permission sets and map them to the existing groups within the company's Active Directory.

Commented [LC96]: https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-sso.html

Question #473

A business that hosts a website on Amazon Web Services (AWS) demands a high degree of scalability, availability, and performance. On Amazon EC2, the firm is operating a Ruby on Rails application. It includes a data tier that runs MySQL 5.6 on Amazon EC2 and is backed up by 16 TB of Amazon EBS storage. Amazon CloudFront is used to cache the content of applications.
The Operations team has reported that the EBS volumes allocated to the MySQL database are growing at a rapid and unexpected rate. The Solutions Architect has been tasked with the responsibility of designing a solution that is highly scalable, highly available, and high-performing.

Which approach is the MOST cost-effective when used to a large 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.

Commented [LC97]: C
A: Not scalable.
B\D: Aurora will auto grow and does not need Lambda. The minimum storage is 10GB. Based on your database usage, your Amazon Aurora storage will automatically grow, up to 64 TB, in 10GB increments with no impact to database performance. There is no need to provision storage in advance.

Question #474 (EXAM)

A business standardized its application deployment process on AWS by using AWS CodePipeline and AWS Cloud Formation. TypeScript and Python are used to write the apps. The firm recently purchased another startup that uses Python scripts to deploy apps to AWS.

Developers at the recently acquired firm are reluctant to migrate their apps to Cloud Formation since doing so would require them to learn a new domain-specific language and remove access to language features such as looping.

How can purchased apps be swiftly brought up to deployment requirements while still addressing the concerns of the developers?

- A. Create Cloud Formation templates and re-use parts of the Python scripts as Instance user data. Use the AWS Cloud Development Kit (AWS CDK) to deploy the application using these templates. Incorporate the AWS CDK into CodePipeline and deploy the application to AWS using these templates.
- B. Use a third-party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired company. Orchestrate the CodeBuild job using CodePipeline.
- C. Standardize on AWS OpsWorks. Integrate OpsWorks with CodePipeline. Have the developers create Chef recipes to deploy their applications on AWS.
- D. Define the AWS resources using TypeScript or Python. Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stacks. Incorporate the AWS CDK as a CodeBuild job in CodePipeline.

Commented [LC98]: https://docs.aws.amazon.com/cdk/v2/guide/home.html

Question #475

A business is deploying its website on AWS. The firm is now working on a variety of security measures that will be implemented on AWS EC2 instances.

Which of the following security measures will not assist the company in preventing future data breaches and identifying security vulnerabilities?

- 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.

Commented [LC99]: 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.

Question #476

A firm created an AWS high performance computing (HPC) cluster for a closely connected application that creates a significant number of shared files stored in Amazon EFS. When the cluster had 100 Amazon EC2 instances, it performed well. When the organization extended the cluster size to 1,000 EC2 instances, however, overall performance was much lower than expected.

Which set of architectural decisions should a solutions architect make in order to maximize the performance of an HPC cluster? (Select three.)

- A. Ensure the HPC cluster is launched within a single Availability Zone.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.
- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the clusters is launched across multiple Availability Zones
- E. Replace Amazon EFS win multiple Amazon EBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

Commented [LC100]: A. High performance computing (HPC) workload cluster should be in a single AZ.
C. Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon EC2 instances to accelerate High Performance Computing (HPC)
F. Amazon FSx for Lustre - Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

Cluster – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Commented [LC101]:

Commented [LC102]:

Question #477

A business operates a legacy system on a single Amazon EC2 instance with Amazon EBS storage that is m4.2xlarge. The web server and a self-managed Oracle database are both operated on the EC2 instance. Every 12 hours, a snapshot of the EBS volume is taken, and an AMI is built from the fully configured EC2 instance.
A recent occurrence caused the EC2 instance to be terminated, resulting in many hours of outage. The application was successfully started from the AMI, however due to the age of the EBS snapshot and the database repair, 8 hours of data were lost. Additionally, the system remained down for four hours while the Systems Operators conducted these tasks manually.

What architectural modifications will help limit downtime and the risk of data loss?

- A. Create an Amazon CloudWatch alarm to automatically recover the instance. Create a script that will check and repair the database upon reboot. Subscribe the Operations team to the Amazon SNS message generated by the CloudWatch alarm.
- B. Run the application on m4.xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of two. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.
- C. Run the application on m4.2xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of one. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.
- D. Increase the web server instance count to two m4.xlarge instances and use Amazon Route 53 round-robin load balancing to spread the load. Enable Route 53 health checks on the web servers. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.

Commented [LC103]: B is correct.
A: Does not address a loss of data since the last backup.
B: Ensures that there are at least two EC instances, each of which is in a different AZ. It also ensures that the database spans multiple AZs. Hence this meets all the criteria.
C: Having auto scaling set to a minimum instance count of one means that if there is just one instance and there is a problem, that instance will need to be restarted, meaning there would an outage during that restart time. As such, B is a better answer.
D: Does not indicate that the two EC2 instances will be in different availability zones. If they are in the same AZ, that entire zone could theoretically have an outage. Given that, I would select B instead of D. Apart from that consideration D does the trick.

Question #478

A business wants to create an online shopping website in various countries and wishes to safeguard clients from possible man-in-the-middle attacks.

Which design will provide the MOST SECURE access to the site?

- 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.

Commented [LC104]: Route53 supports DNSSEC.

See link
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html

Question #479

In the default setup, a corporation has a VPC with two domain controllers running Active Directory. The VPC DHCP options set is configured to utilize the two domain controllers' IP addresses. Although a VPC interface endpoint has been created, instances inside the VPC cannot resolve the private endpoint addresses.

Which techniques would be most effective in resolving this issue? (Select two.)

- A. Define an outbound Amazon Route 53 Resolver. Set a conditional forward rule for the Active Directory domain to the Active Directory servers. Update the VPC DHCP options set to AmazonProvidedDNS.
- B. Update the DNS service on the Active Directory servers to forward all non-authoritative queries to the VPC Resolver.
- C. Define an inbound Amazon Route 53 Resolver. Set a conditional forward rule for the Active Directory domain to the Active Directory servers. Update the VPC DHCP options set to AmazonProvidedDNS.
- D. Update the DNS service on the client instances to split DNS queries between the Active Directory servers and the VPC Resolver.
- E. Update the DNS service on the Active Directory servers to forward all queries to the VPC Resolver.

Commented [LC105]: Should be A and B , as outbound endpoint not necessarily mean that the servers should be onprem for conditional forwarder rule to kick in, instead they can reside in another VPC too and it allows DNS queries from your VPC to the VPC where the AD servers run.
Option C would also work with an inbound endpoint pointing to the 2 AD server IPs, but definitely not with forwarding rules. So clearly ruled out.

Commented [LC106]:

Question #480

A business keeps data about sales transactions in Amazon DynamoDB tables. To promptly discover and react to unusual activity, any changes to the objects contained in DynamoDB tables must be documented within 30 minutes.

Which solution satisfies the criteria?

- A. Copy the DynamoDB tables into Apache Hive tables on Amazon EMR every hour and analyze them for anomalous behaviors. Send Amazon SNS notifications when anomalous behaviors are detected.
- B. Use AWS CloudTrail to capture all the APIs that change the DynamoDB tables. Send SNS notifications when anomalous behaviors are detected using CloudTrail event filtering.
- C. Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda. Create a Lambda function to output records to Amazon Kinesis Data Streams. Analyze any anomalies with Amazon Kinesis Data Analytics. Send SNS notifications when anomalous behaviors are detected.
- D. Use event patterns in Amazon CloudWatch Events to capture DynamoDB API call events with an AWS Lambda function as a target to analyze behavior. Send SNS notifications when anomalous behaviors are detected.

Commented [LC107]: C is correct.

Question #481

A solutions architect is tasked with developing the data storage and retrieval architecture for a new application that a corporation is about to launch. The program is meant to continuously consume millions of tiny records per minute from devices located around the globe. Each record is less than 4 KB in size and must be kept in a persistent place with minimal latency. The data is transient, and the corporation is only obligated to retain it for 120 days before it may be erased.
The solutions architect estimates that the storage needs over the course of a year will be around 10-15 TB.

Which storage technique is the MOST COST-EFFECTIVE and complies with the design specifications?

- A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.
- B. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.
- C. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that executes a query to delete any records older than 120 days.
- D. Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.

Commented [LC108]: A & C - wrong
B - should be correct
D - I am not aware of the API that you can use to search S3 object using used-defined matadata btw. 1.000 put requests cost 0,005 and PUT request header has limitation for user-defined metadata to 2 KB.

Question #482 (EXAM)

Your organization is currently creating a next-generation pet collar that will gather biometric data to aid families in encouraging healthy pet lives. Each collar transmits 30kb of biometric data in JSON format every two seconds to a collecting platform, which processes and analyzes the data and returns health trend information to pet owners and doctors through a web site. Management has assigned you the responsibility of architecting the collection platform while adhering to the following specifications.
⇨ Provide real-time analyses of incoming biometric data
⇨ Ascertain that biometric data processing is very durable. Parallel and elastic
⇨ For data mining purposes, the outputs of analytic processing should be retained.

Which of the following architectures best meets the initial criteria for the collecting platform?

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

Commented [LC109]: B is correct.

Question #483 (SKIP)

Cognito Sync is an Amazon Web Services (AWS) solution that enables you to synchronize user profile data across mobile devices without the need for an in-house backend.

When the gadget is connected to the Internet, data may be synchronized.
What does setting up push sync enable 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

Commented [LC110]: My Answer: C
The question probably won't come up, as AppSync is used now instead of Cognito Sync.

Question #484

A business has developed an application utilizing an in-house software framework. Installation of the framework takes 30 minutes and is carried out using a user data script. The company's developers routinely make improvements to the program. The installation of the framework has become a bottleneck in this procedure.

Which of the following methods would expedite this procedure?

- 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.

Commented [LC111]: A is correct.
B: Does not solve the problem.
C\D: This still does not solve the problem because it still needs 30minutes to install the framework.

Question #485

A Solutions Architect is moving a ten-terabyte PostgreSQL database to Amazon RDS for PostgreSQL using Amazon RDS for PostgreSQL. The company's internet connection is 50 megabytes per second over a VPN in an Amazon VPC, and the Solutions Architect is responsible for migrating data and synchronizing modifications prior to the cutover. The switchover must occur within an eight-day timeframe.

What is the LEAST complicated way for safely and reliably moving the database?

- A. Order an AWS Snowball device and copy the database using the AWS DMS. When the database is available in Amazon S3, use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.
- B. Create an AWS DMS job to continuously replicate the data from on premises to AWS. Cutover to Amazon RDS after the data is synchronized.
- C. Order an AWS Snowball device and copy a database dump to the device. After the data has been copied to Amazon S3, import it to the Amazon RDS instance. Set up log shipping over a VPN to synchronize changes before the cutover.
- D. Order an AWS Snowball device and copy the database by using the AWS Schema Conversion Tool. When the data is available in Amazon S3, use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.

Commented [LC112]: Because A, C and D are unfeasible since the snowball requires more time than 8 days to arrive and come back at AWS.

So it's 50 MBps which means to transfer 10 TB is requires around 2 days.

Question #486

A Solutions Architect is responsible for the design of a data warehousing application's storage layer. Although the data files are enormous, they begin with statically put metadata that indicates the size and location of the file's index. A fleet of Amazon EC2 instances reads the data files in and stores the index size, index position, and other category information about the data file in a database. Amazon EMR makes use of this database to group files together for further analysis.

Which storage system would be the most cost-effective and high-availability 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.

Commented [LC113]: A
Effectively performs a 'ranged' GET request for the part specified. Useful for downloading just a part of an object.
https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectGET.html
B: The maximum throughput you can drive for each NFS client is 250 MB/s. S3 does not have this limit.
C: Can only be mounted on a single instance and not scalable.
D: The file is too large for Dynamo DB.

Question #487

A firm wishes to reorganize their retail ordering online application, which is now hosted on a load-balanced Amazon EC2 instance fleet and uses load-balanced Amazon EC2 instance fleets for web hosting, database API services, and business logic. The organization must develop a decoupled, scalable architecture that includes a method for preserving unsuccessful orders while also keeping operating expenses to a minimum.

Which solution will satisfy these criteria?

- A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use Amazon Elastic Container Service (Amazon ECS) for business logic with Amazon SQS long polling for retaining failed orders.
- B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders.
- C. Use Amazon S3 for web hosting with AWS AppSync for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders.
- D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service (Amazon SES) for order queuing. Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon Elasticsearch Service (Amazon ES) for retaining failed orders.

Commented [LC114]: C is correct.

While AppSync is no better than API GW in this context, the latter part of the answer does mention DLQ which is a "must have"

Question #488

A development team has launched a new aircraft tracker application, providing users with near-real-time data. The application's front end is composed of an Application Load Balancer (ALB) in front of two huge Amazon EC2 instances located in the same Availability Zone. A single Amazon RDS MySQL DB instance is used to store data. A DNS record for Amazon Route 53 links to the ALB.
The development team is tasked with enhancing the solution's dependability while minimizing operating expenses.

Which course of action should be taken by the team?

- A. Create RDS MySQL read replicas. Deploy the application to multiple AWS Regions. Use a Route 53 latency-based routing policy to route to the application.
- B. Configure the DB instance as Multi-AZ. Deploy the application to two additional EC2 instances in different Availability Zones behind an ALB.
- C. Replace the DB instance with Amazon DynamoDB global tables. Deploy the application in multiple AWS Regions. Use a Route 53 latency-based routing policy to route to the application.
- D. Replace the DB instance with Amazon Aurora with Aurora Replicas. Deploy the application to multiple smaller EC2 instances across multiple Availability Zones in an Auto Scaling group behind an ALB.

Commented [LC115]: A. possible, but if something happen there is a lot of operational work to do (ex : promoting read replica. and also this one is not very certain since read replica will replicate inside region unless you configure it to global read replica
B. adding 2 additional Ec2 is not correct and not best practice. its vertical scaling , and aws suggest to use horizontal scaling
C. Not every database suit DynamoDb , will choose this if they say more about the data structure
D. Aurora is managed. This one is the best over all the choices.

Question #489

How does AWS Data Pipeline perform operations on on-premises or managed AWS resources?

- A. By supplying a Task Runner package that can be installed on your on-premise hosts
- B. None of these
- C. By supplying a Task Runner file that the resources can access for execution
- D. By supplying a Task Runner json script that can be installed on your on-premise hosts

Commented [LC116]: To enable running activities using on-premise resources, AWS Data Pipeline does the following: It supply a Task Runner package that can be installed on your on- premise hosts. This package continuously polls the AWS Data Pipeline service for work to perform. When it's time to run a particular activity on your on-premise resources, it will issue the appropriate command to the Task Runner.

Reference:

https://aws.amazon.com/datapipeline/faqs/

Question #490

You're operating an application on-premises owing to its reliance on non-x86 hardware and would want to backup your data using AWS. Your backup program can only write to block-based storage that is POSIX-compatible. You have 140TB of data and want to mount it on your file server as a single folder. Users must be able to access sections of this data during backups.

Which backup option would be the best fit for this scenario?

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

Commented [LC117]: Since it says "sections" of data, I'm inclined to pick A.

Question #491

A solutions architect is tasked with the responsibility of developing a disaster recovery plan for a three-tiered application. The application's data layer has an RTO of 30 minutes and an RPO of 5 minutes. The application and web layers are stateless and run on an Amazon EC2 fleet of instances. The data layer is comprised of an Amazon Aurora database with a capacity of 50 TB.

Which sequence of procedures best achieves the RTO and RPO criteria while being cost effective? (Select two.)

- A. Create daily snapshots of the EC2 instances and replicate the snapshots to another Region.
- B. Deploy a hot standby of the application to another Region.
- C. Create snapshots of the Aurora database every 5 minutes.
- D. Create a cross-Region Aurora Replica of the database.
- E. Create an AWS Backup job to replicate data to another Region.

Commented [LC118]: A correct - if an application will be changed it is good to have its most current release
B wrong - not needed, even for largest instances initialization of a new server will be shorter than 10 minutes
C wrong - doesn't mention another Region btw. have you ever done snapshot on a database with this size.
Restrictions:
- automatic backup frequency - 1 day
- manual snapshots - 100 cluster snapshots and 100 db snapshots. It can be adjusted but the answer is not mentioning it.
D correct
E wrong - is not usable in this scenario

Commented [LC119]:

Question #492

Your organization is about to make a significant public announcement about a social networking platform hosted on AWS. The website is hosted on Amazon EC2 instances that are distributed across different Availability Zones and are connected to a Multi-AZ RDS MySQL Extra Large DB Instance. The site does a large volume of tiny reads and writes per second and uses an eventual consistency mechanism. You notice that there is read contention on RDS MySQL after doing extensive testing.

Which techniques are the most effective in meeting these requirements? (Select 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

Commented [LC120]:

Commented [LC121]:

Question #493

Your client is interested in consolidating their log streams (access logs, application logs, and security logs, among others) into a single system. Once aggregated, the client wants to do real-time analysis of these logs using heuristics. Occasionally, the client will need to check heuristics, which will necessitate reverting to data samples gathered within the recent 12 hours.

What is the most effective strategy for meeting 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

Commented [LC122]: Since it's 'real-time' analysis, my chances are on B.

Question #494

A business employs a three-tiered architecture with two Availability Zones. Users say that the website is down during the company's off season. The Solutions Architect determines that there have been no recent modifications to the environment, that the website is accessible, and that logging in is feasible. When the Solutions Architect chooses the "find a shop near you" feature, the maps offered on the site through a third-party RESTful API request fail to operate around 50% of the time after refreshing the page. Outbound API calls are routed using Amazon EC2 Network Address Translation (NAT) instances.

Which of the following is the MOST LIKELY cause of this failure, and how may it be avoided 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.

Commented [LC123]: The issue is 50% failure, means the balancing over 2 AZs is failing on one NAT instance in one AZ. The solution is to replace the NAT instance with fully managed and high available NAT gateway.

Question #495

Which of the following assertions regarding AWS Direct Connect is correct?

- 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.

Commented [LC124]: B is actually correct.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

An AWS Direct Connect location provides access to AWS in the Region with which it is associated
https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

You can create a Direct Connect gateway in any public Region. Use it to connect your AWS Direct Connect connection over a private virtual interface to VPCs in your account that are located in different Regions or to a transit gateway. For more information, see Working with Direct Connect gateways.

Question #496

Your organization's rules mandate the encryption of sensitive data in transit. You're weighing your choices for data protection while it's stored at rest on an EBS data disk connected to an EC2 instance.

Which of the following choices enables you to encrypt your data in transit? (Select three.)

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

Commented [LC125]: Wired question to make you fail. This is a very bad written question. It wants to know how to encrypt AT REST, not in transit.

It's A, C, D.

B is in transit.
E is wrong.

Commented [LC126]:

Commented [LC127]:

Question #497

A business is now utilizing AWS CodeCommit as its source control system and AWS CodePipeline as its continuous integration platform. The pipeline includes a build step for generating artifacts, which are subsequently stored in an Amazon S3 bucket.
The organization has discovered several possibilities for process improvement and has assigned the following criteria to a Solutions Architect:
⇨ Establish a new pipeline to facilitate feature development.
⇨ Sustain feature development while minimizing effect on production applications
⇨ Continuous testing should be integrated with unit testing.
⇨ Separate development and manufacturing artifacts
⇨ Sustain the capability of integrating testing and production code.

How should the Solutions Architect accomplish these goals?

- A. Trigger a separate pipeline from CodeCommit feature branches. Use AWS CodeBuild for running unit tests. Use CodeBuild to stage the artifacts within an S3 bucket in a separate testing account.
- B. Trigger a separate pipeline from CodeCommit feature branches. Use AWS Lambda for running unit tests. Use AWS CodeDeploy to stage the artifacts within an S3 bucket in a separate testing account.
- C. Trigger a separate pipeline from CodeCommit tags. Use Jenkins for running unit tests. Create a stage in the pipeline with S3 as the target for staging the artifacts with an S3 bucket in a separate testing account.
- D. Create a separate CodeCommit repository for feature development and use it to trigger the pipeline. Use AWS Lambda for running unit tests. Use AWS CodeBuild to stage the artifacts within different S3 buckets in the same production account.

Commented [LC128]:

Question #498

A business that manages job listings for seasonal workers has seen an increase in traffic and utilization. The backend services are hosted on a pair of Amazon EC2 instances behind an Application Load Balancer, with the datastore being Amazon DynamoDB. During high seasons, application read and write traffic is sluggish.

Which option requires the LEAST effort in terms of development work for a scalable application architecture capable of handling peak seasons?

- A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB
- B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables
- C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling
- D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB

Commented [LC129]: Key is LEAST effort. Answer is C.

Question #499

Someone is establishing a virtual private cloud (VPC) for the purpose of hosting an application. He's constructed two private subnets inside the same availability zone and one in a different availability zone. He wants to build a High Availability system that has an internal Elastic Load Balancer.

Which of the following statements is true in this circumstance involving internal ELBs? (Select 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.

Commented [LC130]: Answer is A & C,

D also possible only if you enable Cross-Zone Load Balancing

If cross-zone load balancing is enabled, each node is connected to each back-end instance, regardless of Availability Zone. Otherwise, each node is connected only to the instances that are in its Availability Zone.

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-internal-load-balancers.html

Commented [LC131]:

Questions 500-599

Question #500 (EXAM)

Recently, a firm migrated from conventional infrastructure provisioning scripts to AWS CloudFormation templates. The freshly produced templates are available for download through the company's private GitHub repository. Since using CloudFormation, the organization has seen multiple difficulties with template upgrades causing execution or environment creation to fail. The surge in mistakes has prompted management to hire a Solutions Architect to create automated testing for CloudFormation template upgrades.

What actions should the Solution Architect take to ensure that these criteria are met?

- A. Use AWS CodePipeline to create a change set from the CloudFormation templates stored in the private GitHub repository. Execute the change set using AWS CodeDeploy. Include a CodePipeline action to test the deployment with testing scripts run by AWS CodeBuild.
- B. Mirror the GitHub repository to AWS CodeCommit using AWS Lambda. Use AWS CodeDeploy to create a change set from the CloudFormation templates and execute it. Have CodeDeploy test the deployment with testing scripts run by AWS CodeBuild.
- C. Use AWS CodePipeline to create and execute a change set from the CloudFormation templates stored in the GitHub repository. Configure a CodePipeline action to test the deployment with testing scripts run by AWS CodeBuild.
- D. Mirror the GitHub repository to AWS CodeCommit using AWS Lambda. Use AWS CodeBuild to create a change set from the CloudFormation templates and execute it. Have CodeBuild test the deployment with testing scripts.

Commented [LC132]: https://aws.amazon.com/blogs/devops/building-a-ci-cd-pipeline-to-update-an-aws-cloudformation-stacksets/

Codepipeline can use as a source Github so B, D are ruled out.

Difference between Code Pipeline and Code Deploy:

https://stackshare.io/stackups/aws-codedeploy-vs-aws-codepipeline#:~:text=CodePipeline%20builds%2C%20tests%2C%20and%20deploys,classified%20under%20%22Continuous%20Deployment%22

https://docs.aws.amazon.com/codepipeline/latest/userguide/connections-github.html

Question #501

If a condition in an IAM policy has many values for a single key, the condition will be assessed using a logical _____.

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

Commented [LC133]: A is correct.

Ref.
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_multi-value-conditions.html

Question #502

A customer-managed AWS Identity and Access Management (IAM) policy has been applied to the following IAM user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": [
          "arn:aws:s3:::prod-data",
          "arn:aws:s3:::prod-data/*"
        ]
    },
    {
        "Effect":"Deny",
        "NotAction": "s3:*",
        "NotResource": [
          "arn:aws:s3:::prod-data",
          "arn:aws:s3:::prod-data/*"
        ]
    }
  ]
}
```


Which statement best characterizes the access granted to the user by this policy?

- A. The policy grants access to all Amazon S3 actions, including all actions in the prod-data S3 bucket
- B. This policy denies access to all Amazon S3 actions, excluding all actions in the prod-data S3 bucket
- C. This policy denies access to the Amazon S3 bucket and objects not having prod-data in the bucket name
- D. This policy grants access to all Amazon S3 actions in the prod-data S3 bucket, but explicitly denies access to all other AWS services

Commented [LC134]: Answer: D

NotAction + NotResource
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_notaction.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_notresource.html

Question #503

Which of the following rules must be applied to a mount target security group in order for an on-premises server to access Amazon Elastic File System (EFS)?

- 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.

Commented [LC135]: 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.

Reference:
http://docs.aws.amazon.com/efs/latest/ug/how-it-works.html

Question #504

You've configured Auto Scaling to scale in automatically. As a result, you must choose which instances of Auto Scaling should be terminated first.

How should this be configured?

- A. An Elastic Load Balancer
- B. A termination policy
- C. An IAM role
- D. Another scaling group

Commented [LC136]: If you instruct Auto Scaling to automatically scale in, you must decide which instances Auto Scaling should terminate first. This can be configured through the use of a termination policy.

Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingBehavior.InstanceTermination.html

Question #505

A Solutions Architect is developing a solution for web servers to update user information. In less than 30 seconds, the solution must scale from hundreds to tens of thousands of employments. The remedy must be asynchronous, perpetually avoidable, and cost-effective.

Which tactics should the Solutions Architect use to achieve these objectives?

- A. Create an AWS SWF worker that will update user metadata updating web application to start a new workflow for every job.
- B. Create an AWS Lambda function that will update user metadata. Create an Amazon SQS queue and configure it as an event source for the Lambda function. Update the web application to send jobs to the queue.
- C. Create an AWS Lambda function that will update user metadata. Create AWS Step Functions that will trigger the Lambda function. Update the web application to initiate Step Functions for every job.
- D. Create an Amazon SQS queue. Create an AMI with a worker to check the queue and update user metadata. Configure an Amazon EC2 Auto Scaling group with the new AMI. Update the web application to send jobs to the queue.

Commented [LC137]: Since this is a just a simple job to update the metadata, I would eliminate workflow options such as A and C. Between B and D I would chose B because it will be easier to scale with Lambda using SQS as an event source as per the requirement than it is with EC2 Auto scaling.

Question #506

A solutions architect is tasked with the responsibility of developing a network for a new cloud deployment. Each account will need autonomy to alter and update route tables. Additionally, centralized and regulated internet access is required for egress. The cloud footprint is likely to expand to thousands of Amazon Web Services (AWS) customers.

Which architecture will satisfy these criteria?

- A. A centralized transit VPC with a VPN connection to a standalone VPC in each account. Outbound internet traffic will be controlled by firewall appliances.
- B. A centralized shared VPC with a subnet for each account. Outbound internet traffic will be controlled through a fleet of proxy servers.
- C. A shared services VPC to host central assets to include a fleet of firewalls with a route to the internet. Each spoke VPC will peer to the central VPC.
- D. A shared transit gateway to which each VPC will be attached. Outbound internet access will route through a fleet of VPN-attached firewalls.

Commented [LC138]: Looks like D.

Answer C is wrong, because there is a default limit of 50 VPS peerings per VPC, which can be increased to a maximum of 125.

Ref.
https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

Since the cloud footprint is expected to grow to thousands of AWS accounts, VPC peering with one central VPC would not work. Transit Gateway can handle up to 5000 attachments and therefore is the better choice here.

Question #507

You've been tasked with designing an application's storage layer. The program demands a minimum of 100,000 IOPS from the disk. Additionally, the storage layer must be capable of surviving the loss of a single disk, EC2 instance, or Availability Zone without compromising data integrity. The volume you provide must have a minimum capacity of 3 TB.

Which of the following designs will accomplish these goals?

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

Commented [LC139]: Answer is E
Keyword is "or Availability Zone without any data loss"

A: RAID 5 is not recommened by AWS. Also need replicate to another AZ

B: Need synchronous replication to prevent any data loss (in case lost AZ)

C: Need synchronous replication to prevent any data loss

D: Need synchronous replication to prevent any data loss

Question #508

A corporation is considering moving mission-critical applications from an on-premises data center to AWS. The organization has a Microsoft SQL Server Always On cluster installed on-premises. The business wishes to switch to an Amazon Web Services managed database service. A solutions architect is tasked with the responsibility of designing a heterogeneous database migration on AWS.

Which solution will satisfy these criteria?

- A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.
- B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.
- C. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.
- D. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQL. Use S3 integration with SQL Server features, such as BULK INSERT.

Commented [LC140]: There's Microsoft SQL Server on RDS but none of the questions provides it. It's C, it requires a conversion between heterogeneous systems.

Ref. https://aws.amazon.com/dms/schema-conversion-tool/

Question #509

Recently, a firm in the United Kingdom (UK) achieved a successful proof of concept on Amazon WorkSpaces. Additionally, the corporation maintains a sizable presence in the United States (US). Each office's staff employees move between the two sites on a regular basis and want access to a corporate WorkSpace without reconfiguring their WorkSpaces client.

The organization acquired a domain and created a connection alias using Amazon Route 53. The organization will implement a Windows profile and document management system.

A solutions architect is required to create the whole solution. The solution must use a WorkSpace architecture in two AWS Regions and must include regional resilience.

Which solution will satisfy these criteria?

- A. Create a connection alias in a UK Region and a US Region. Associate the connection alias with a directory in the UK Region. Configure the DNS service for the domain in the connection alias. Configure a geolocation routing policy. Distribute the connection string to the WorkSpaces users.
- B. Create a connection alias in a UK Region. Associated the connection alias with a directory in the UK Region. Configure the DNS service for the domain in the connection alias. Configure a weighted routing policy, with the UK Region set to 1 and a US Region set to 255. Distribute the connection string for the UK Region to the WorkSpaces users.
- C. Create a connection alias in a UK Region and a US Region. Associate the connection aliases with a directory in each Region. Configure the DNS service for the domain in the connection alias. Configure a geolocation routing policy. Distribute the connection string to the WorkSpaces users.
- D. Create a connection alias in a US Region. Associated the connection alias with a directory in the UK Region. Configure the DNS service for the domain in the connection alias. Configure a multivalue answer routing policy. Distribute the connection string for the US Region to the WorkSpaces users.

Commented [LC141]: https://docs.aws.amazon.com/workspaces/latest/adminguide/cross-region-redirection.html

Question #510

AWS Organizations is being used to manage 15 AWS accounts by a business. A solutions architect wishes to do sophisticated analytics on the cloud expenses of his organization. Cost information must be collected and made accessible via an analytics account. The analytics program is hosted in a VPC and requires raw cost data each night to execute.

The solutions architect has chosen to use the Cost Explorer API to get the raw data and save it in JSON format in Amazon S3. The analytics program must have exclusive access to the raw cost data. The architect of the solution has already established an AWS Lambda function to gather data using the Cost Explorer API.

Which further steps should the solutions architect take to ensure compliance with these requirements?

- A. Create an IAM role in the Organizations master account with permissions to use the Cost Explorer API, and establish trust between the role and the analytics account. Update the Lambda function role and add sts:AssumeRole permissions. Assume the role in the master account from the Lambda function code by using the AWS Security Token Service (AWS STS) AssumeRole API call. Create a gateway endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the S3 endpoint.
- B. Create an IAM role in the analytics account with permissions to use the Cost Explorer API. Update the Lambda function and assign the new role. Create a gateway endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the analytics VPC by using the aws:SourceVpc condition.
- C. Create an IAM role in the Organizations master account with permissions to use the Cost Explorer API, and establish trust between the role and the analytics account. Update the Lambda function role and add sts:AssumeRole permissions. Assume the role in the master account from the Lambda function code by using the AWS Security Token Service (AWS STS) AssumeRole API call. Create an interface endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the analytics VPC private CIDR range by using the aws:SourceIp condition.
- D. Create an IAM role in the analytics account with permissions to use the Cost Explorer API. Update the Lambda function and assign the new role. Create an interface endpoint for Amazon S3 in the analytics VPC. Create an S3 bucket policy that allows access only from the S3 endpoint.

Commented [LC142]: Agreed, A is correct. C could be correct except for the part about restricting access using a bucket policy with aws:SourceIp which leaves A.

Ref.
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html#vpc-endpoints-s3-bucket-policies

Question #511

A Solutions Architect is constructing a containerized .NET Core application for AWS Fargate. The application's backend needs a high-availability version of Microsoft SQL Server. All application levels must be extremely accessible. The credentials associated with the SQL Server connection string should not be saved to disk inside the .NET Core front-end containers.

Which tactics should the Solutions Architect use to achieve these objectives?

- A. Set up SQL Server to run in Fargate with Service Auto Scaling. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server running in Fargate. Specify the ARN of the secret in AWS Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
- B. Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
- C. Create an Auto Scaling group to run SQL Server on Amazon EC2. Create a secret in AWS Secrets Manager for the credentials to SQL Server running on EC2. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server on EC2. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.
- D. Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create non-persistent empty storage for the .NET Core containers in the Fargate task definition to store the sensitive information. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be written to the non-persistent empty storage on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

Commented [LC143]: B. Secrets Manager natively supports SQL Server on RDS. No real need to create additional 'ephemeral storage' to fetch credentials, as these can be injected to containers as environment variables.

A and C are wrong because the DB should run on RDS.

https://aws.amazon.com/premiumsupport/knowledge-center/ecs-data-security-container-task/

Question #512

Your team has a Java application built on Tomcat that has to be deployed to development, test, and production environments. You decide to utilize Elastic Beanstalk owing to its strong connection with your development tools and RDS due to its simplicity of administration after doing some study. Your QA team's lead informs you that you must nightly roll a sanitized set of production data into your environment. Likewise, other software teams within your organization need access to the recovered data through their EC2 instances inside your VPC.
The following is the ideal persistence and security configuration that satisfies the aforementioned parameters.

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

Commented [LC144]: It can't be A because the scenario specifically requires persistence. According to http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.db.html "A database instance that is part of your environment is tied to the lifecycle of your environment. If you terminate the environment, the database instance is terminated as well. An integrated database instance also cannot be removed from your environment once added."

It can't be B because we never have access to the IP address of any RDS instance.

C & D are very similar except that the scenario requirements specifically state that optimal security should be applied.

It can't be D because RDS is opened to all "hosts in your application subnets" where C only opens RDS to specific client machines in a specific security group.

C is the correct answer.

Question #513

You have a periodic image analysis program that accepts files as input, analyzes them, and publishes data from each file to a ten-file output. The number of files received each day is high and concentrated in a few hours of the day. At the moment, you have an EC2 server with a huge EBS volume hosting the input data and the results. The procedure takes over 20 hours every day to finish.

What services might be employed to shorten the solution's development time and increase its availability?

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

Commented [LC145]:

Question #514

Requests for auto scaling are accompanied with a _____ signature computed using the request's parameters and the user's private key.

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

Commented [LC146]: https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

Question #515

You used Elastic Beanstalk to launch your corporate website and configured log file rotation to S3. An Elastic Map Reduce task analyzes the logs on S3 on a periodic basis to create a usage dashboard that you can share with your CIO.
You recently enhanced the website's overall performance by using Cloud Front for dynamic content delivery and your own domain as the origin. Following this architectural modification, the use dashboard indicates that your website's traffic decreased by an order of magnitude.

How can you correct a problem with your use dashboard?

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

Commented [LC147]: Should be A.

Ref.
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html#access-logs-choosing-s3-bucket

Question #516

Which of the following is a function of Amazon DynamoDB?

- 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

Commented [LC148]: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithItems.html#WorkingWithItems.AtomicCounters

Question #517

A business is running a legacy application on Amazon EC2 instances distributed across several Availability Zones and protected by a software load balancer operating on an active/standby set of EC2 instances. The organization has established a warm standby replica of the application environment that is deployed in another AWS Region for disaster recovery purposes. The application's domain is hosted via Amazon Route 53.

The business requires that the application utilize static IP addresses, even during a failover to the backup Region. Additionally, the organization wants access to the client's originating IP address for auditing reasons.

Which method satisfies these criteria with the FASTEST operational overhead?

- A. Replace the software load balancer with an AWS Application Load Balancer. Create an AWS Global Accelerator accelerator. Add an endpoint group for each Region. Configure Route 53 health checks. Add an alias record that points to the accelerator.
- B. Replace the software load balancer with an AWS Network Load Balancer. Create an AWS Global Accelerator accelerator. Add an endpoint group for each Region. Configure Route 53 health checks. Add a CNAME record that points to the DNS name of the accelerator.
- C. Replace the software load balancer with an AWS Application Load Balancer. Use AWS Global Accelerator to create two separate accelerators. Add an endpoint group for each Region. Configure Route 53 health checks. Add a record set that is configured for active-passive DNS failover. Point the record set to the DNS names of the two accelerators.
- D. Replace the software load balancer with an AWS Network Load Balancer. Use AWS Global Accelerator to create two separate accelerators. Add an endpoint group for each Region. Configure Route 53 health checks. Add a record set that is configured for weighted round-robin DNS failover. Point the record set to the DNS names of the two accelerators.

Commented [LC149]: A global accelerator supports multiple endpoints in different regions, which can be ALBs or NLBs, so two accelerators are not required. This leaves only A and B. Also, alias are an aws dns record so it's more liked by AWS.

Between A and B, A is the better option as its easier to preserve the client IP with an ALB.

Answer: A

See - https://docs.aws.amazon.com/global-accelerator/latest/dg/getting-started.html#getting-started-add-endpoints

Question #518

On AWS's us-east-1 Region, a business runs a web application. Behind an Application Load Balancer, the application servers are deployed across three Availability Zones. The database is hosted on an Amazon EC2 instance using a MYSQL database. A solutions architect must develop a cross-Region data recovery solution that leverages AWS services and has an RTO of fewer than 5 minutes and an RPO of less than 1 minute. The solutions architect has deployed application servers in us-west-2 and implemented health checks and DNS failover to us-west-2 using Amazon Route 53.

Which extra step is necessary for the solutions architect?

- A. Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2.
- B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.
- C. Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.
- D. Create a MySQL standby database on an Amazon EC2 instance in us-west-2.

Commented [LC150]: https://aws.amazon.com/rds/aurora/global-database/

Question #519

A business is deploying a website on the AWS VPC. To stave against a D-DOS assault, the organization has blacklisted a few IP addresses.

How can an organization ensure that requests from the aforementioned IP addresses are denied access to 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.

Commented [LC151]:

Question #520

True or False: At the moment, Amazon ElastiCache clusters are not accessible in VPC.

- A. TRUE
- B. True, but they are available only in the GovCloud.
- C. True, but they are available only on request
- D. FALSE

Commented [LC152]: 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. Reference: http://aws.amazon.com/about-aws/whats-new/2012/12/20/amazon-elasticache-announces-support-for-amazon-vpc/

Question #521 (EXAM)

A company's industrial and automation apps are hosted in a single virtual private cloud (VPC). Over twenty apps are hosted on a mix of Amazon EC2, Amazon Elastic Container Service (Amazon ECS), and Amazon Relational Database Service (Amazon RDS).

The organization has three teams of software developers. Each application is owned by one of the three teams, and each team is responsible for the cost and performance of all of its applications. Team resources include tags that identify them as belonging to their application or team. The teams rely on IAM access for day-to-day operations.

The organization must establish which AWS charges are attributed to specific applications or teams on a monthly basis. Additionally, the business must be able to provide reports that compare expenditures from the previous 12 months and assist in forecasting costs for the upcoming 12 months. A solutions architect must suggest an AWS Billing and Cost Management solution capable of generating these cost reports.

Which combination of acts satisfies these criteria? (Select three.)

- A. Activate the user-define cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

Commented [LC153]: A. After you create and apply user-defined tags, you can activate them for cost allocation.

D. By default, IAM users don't have access to the AWS Billing and Cost Management console. You or your account administrator must grant users' access.

F. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase.

Question #522

A user wishes to host a Highly Available system on the AWS Virtual Private Cloud.

Which of the following assertions is true in this situation?

- A. Create VPC subnets in two separate availability zones and launch instances in different subnets.
- B. Create VPC with only one public subnet and launch instances in different AZs using that subnet.
- C. Create two VPCs in two separate zones and setup failover with ELB such that if one VPC fails it will divert traffic to another VPC.
- D. Create VPC with only one private subnet and launch instances in different AZs using that subnet.

Commented [LC154]:

Commented [LC155]:

Commented [LC156]:

Question #523

Your client intends to install an enterprise application on AWS, which will include several web servers, multiple application servers, and a modest (50GB) Oracle database. The database and the file systems of the multiple servers are used to store information. The backup system must allow database recovery, including full server and disk restorations, as well as individual file restores with a maximum recovery time of two hours. They've picked Oracle RDS as the database platform.

Which backup architecture will satisfy these criteria?

- 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.

Commented [LC157]: Answer is A
B: Multi-AZ is more of a Disaster recovery solution
C: Glacier not an option with the 2 hours RTO
D: Will use RMAN only if Database hosted on EC2 and not when using RDS

Question #524

A business has developed a web application that enables users to post brief films. The videos are saved on Amazon EBS volumes and are classified using bespoke recognition software.
The website includes static material and receives sporadic visitation throughout specific months. The architecture is composed of Amazon EC2 instances operating in an Auto Scaling group for the web application and EC2 instances processing an Amazon SQS queue. The firm want to re-architect the application in order to decrease operational expenses via the use of AWS managed services and to eliminate reliance on third-party software.

Which solution satisfies these criteria?

- A. Use Amazon ECS containers for the web application and Spot instances for the Scaling group that processes the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.
- B. Store the uploaded videos in Amazon EFS and mount the file system to the EC2 instances for the web application. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- C. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notification to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that call the Amazon Rekognition API to categorize the videos.
- D. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

Question #525

A business runs a service for matching game players on a publicly accessible, physical, on-premises instance that all users may access over the internet. UDP is used for all traffic to and from the instance. The organization want to shift the service to Amazon Web Services (AWS) and ensure a high degree of security. A solutions architect is required to create an AWS-based solution for the player-matching service.

Which measures should the solutions architect do in combination to satisfy these requirements? (Select three.)

- A. Use a Network Load Balancer (NLB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the NLB's Elastic IP address.
- B. Use an Application Load Balancer (ALB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the ALB's internet- facing fully qualified domain name (FQDN).
- C. Define an AWS WAF rule to explicitly drop non-UDP traffic, and associate the rule with the load balancer.
- D. Configure a network ACL rule to block all non-UDP traffic. Associate the network ACL with the subnets that hold the load balancer instances.
- E. Use Amazon CloudFront with an Elastic Load Balancer as an origin.
- F. Enable AWS Shield Advanced on all public-facing resources.

Question #526

A business wishes to use Amazon S3 for the purpose of backing up its on-premises file storage system. The company's on-premises file storage solution supports NFS, and the new solution should as well. After five days, the corporation wishes to archive the backup files. If a business need archived data for catastrophe recovery, it is willing to wait a few days for their retrieval.

Which option best fits these criteria in terms of cost-effectiveness?

- A. Deploy an AWS Storage Gateway files gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the file to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.
- C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- D. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- E. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

Commented [LC158]:

Commented [LC159]: A, D, F is perfect answer

The Network Load Balancer (NLB) supports the UDP protocol and can be placed in front of the application instance.
This configuration may add some security if the instance is running in a private subnet.

An NLB can be configured with an Elastic IP in each subnet in which it has nodes. In this case it only has a single subnet (one instance) and so there will be 1 EIP.

Route 53 can be configured to resolve directly to the EIP rather than the DNS name of the NLB as there is only one IP address to return.

To filter traffic the network ACL for the subnet can be configured to block all non-UDP traffic.

This solution meets all the stated requirements.

Commented [LC160]:

Commented [LC161]: WAF can't be put in front of NLB.

Commented [LC162]: The Amazon S3 File Gateway enables you to store and retrieve objects in Amazon S3 using file protocols such as Network File System (NFS) and Server Message Block (SMB). Objects written through S3 File Gateway can be directly accessed in S3.

The Amazon FSx File Gateway enables you to store and retrieve files in Amazon FSx for Windows File Server using the SMB protocol. Files written through Amazon FSx File Gateway are directly accessible in Amazon FSx for Windows File Server.
The Volume Gateway provides block storage to your on-premises applications using iSCSI connectivity. Data on the volumes is stored in Amazon S3 and you can take point in time copies of volumes which are stored in AWS as Amazon EBS snapshots. You can also take copies of volumes and manage their retention using AWS Backup. You can restore EBS snapshots to a Volume Gateway volume or an EBS volume.

The Tape Gateway provides your backup application with an iSCSI virtual tape library (VTL) interface, consisting of a virtual media changer, virtual tape drives, and virtual tapes. Virtual tapes are stored in Amazon S3 and can be archived to Amazon S3 Glacier or Amazon S3 Glacier Deep Archive.

Question #527

You are responsible for building an intrusion detection and prevention system (IDS/IPS) solution for a client web application inside a single VPC. You are weighing the pros and downsides of deploying IOS IPS protection for Internet traffic.

Which of the following are you considering? (Select 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.

Commented [LC163]: EC2 does not allow promiscuous mode, and you cannot put something in between the ELB and the web server (like a listener or IDP)

Commented [LC164]:

Question #528

Determine one advantage of implementing Auto Scaling in your application.

- A. Your application gains better fault tolerance.
- B. Your application optimizes only logistics and operations.
- C. Your application receives latency requirements in every region.
- D. You acquire clarity on prototypes in your application.

Commented [LC165]: When you use Auto Scaling, your applications gain better fault tolerance. Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. You can also configure Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Auto Scaling can launch instances in another one to compensate.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/how-as-works.html

Question #529

A business operates an application on a fleet of Amazon EC2 instances and saves 70 GB of device data in Amazon S3 for each instance. Recently, some S3 uploads have failed. Simultaneously, the organization is seeing an unanticipated spike in data storage expenses. Modifications to the application's code are not permitted.

What is the MOST EFFECTIVE method for uploading device data to Amazon S3 while keeping storage costs in check?

- A. Upload device data using a multipart upload. Use the AWS CLI to list incomplete parts to address the failed S3 uploads. Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating.
- B. Upload device data using S3 Transfer Acceleration. Use the AWS Management Console to address the failed S3 uploads. Use the Multi-Object Delete operation nightly to delete the old uploads.
- C. Upload device data using a multipart upload. Use the AWS Management Console to list incomplete parts to address the failed S3 uploads. Configure a lifecycle policy to archive continuously to Amazon S3 Glacier.
- D. Upload device data using S3 Transfer Acceleration. Use the AWS Management Console to list incomplete parts to address the failed S3 uploads. Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating.

Commented [LC166]: "Use the AWS Management Console to list incomplete parts to address the failed S3 uploads" - not possible with Management Console
C & D - wrong
"Upload device data using S3 Transfer Acceleration" - can be used to move data between Regions. Not in this case
B & D - wrong
"Use the AWS Management Console to address the failed S3 uploads." - there is no functionality
B - wrong
"Use the AWS CLI to list incomplete parts to address the failed S3 uploads" - correct
"Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating." - correct
A - correct. I assume that they will not change the application and use CLI to upload files

Question #530

On AWS, a corporation hosts an image-processing service in a VPC. The Virtual Private Cloud spans two Availability Zones. Each Availability Zone is comprised of a public and a private subnet.

The service is implemented using Amazon EC2 instances on private subnets. In the public subnets, an Application Load Balancer is in front of the service. The service requires internet connectivity, which it does through two NAT gates. The service stores images on Amazon S3. Each day, the EC2 instances download around 1' of data from an S3 bucket.

The firm touts the service as very secure. A solutions architect's objective is to minimize cloud expenditures while maintaining the service's security posture and minimizing time spent on ongoing operations.

Which solution will satisfy these criteria?

- A. Replace the NAT gateways with NAT instances. In the VPC route table, create a route from the private subnets to the NAT instances.
- B. Move the EC2 instances to the public subnets. Remove the NAT gateways.
- C. Set up an S3 gateway VPC endpoint in the VPC. Attach an endpoint policy to the endpoint to allow the required actions on the S3 bucket.
- D. Attach an Amazon Elastic File System (Amazon EFS) volume to the EC2 instances. Host the image on the EFS volume.

Commented [LC167]: Create Amazon S3 gateway endpoint in the VPC and add a VPC endpoint policy. This VPC endpoint policy will have a statement that allows S3 access only via access points owned by the organization.

Question #531

A business hosts a three-tier web application on-premises. Due to a recent spike in traffic that resulted in downtime and a major financial effect, the application's management has directed that it be migrated to AWS. The program is developed in .NET and is MySQL-reliant. A solutions architect must create a scalable and highly available system that can support the daily demands of 200,000 users.

Which actions should the solutions architect follow in order to build a solution that is appropriate?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.
- C. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- D. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

Commented [LC168]: A, C: Elastic beanstalk are regional. All Beanstalk resources of one environment are located only in one region. This means you cannot run an instance in Frankfurt and one in Ohio, but you can run those in multiple availability zones for one region.
D: no spot instance. No HA for the DB.

Question #532

Which of the following should be the last step before beginning to use AWS Direct Connect?

- A. Creating your Virtual Interface
- B. Configuring your router
- C. Completing the Cross Connect
- D. Verifying your Virtual Interface

Commented [LC169]: 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

Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#connected

Question #533

A web application is hosted in a dedicated VPC that is linked by a Site-to-Site VPN to the company's on-premises data center. The application is only available over the corporate network. This is a non-production, temporary application that is only utilized during business hours. The workload is typically light, with brief spikes.
On the backend, the application uses an Amazon Aurora MySQL supplied database cluster. The VPC is equipped with an internet gateway and NAT gateways.
The web servers are located in private subnets behind an Elastic Load Balancer in an Auto Scaling group. Additionally, the web servers transfer data to an Amazon S3 bucket through the internet.
A solutions architect's primary objective should be to minimize operating expenses and to simplify the design.

Which approach should be used by the solutions architect?

- A. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Use 3-year scheduled Reserved Instances for the web server EC2 instances. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket.
- B. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
- C. Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only. Detach the internet gateway from the VPC, and use an Aurora Serverless database. Set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes.
- D. Use 3-year scheduled Reserved Instances for the web server Amazon EC2 instances. Remove the NAT gateways from the VPC, and set up a VPC endpoint for the S3 bucket. Use Amazon CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours only. Update the network routing and security rules and policies related to the changes.

Commented [LC170]: An Internet gateway is not required to establish a Site-to-Site VPN connection, a Customer Gateway is necessary.

Ref:
https://aws.amazon.com/vpn/faqs/#:~:text=Amazon%20supports%20Internet%20Protocol%20security,-to-Site%20VPN%20connection.

Question #534

A business hosts a legacy application on an Amazon EC2 instance inside a VPC that does not have internet connectivity. The application is accessed by users through a desktop software installed on their workplace laptops. The laptops communicate with the VPC through AWS Direct Connect (DX). A new requirement says that all data in transit between users and the VPC must be encrypted.

Which method should a solutions architect use to ensure that network performance remains constant while satisfying this new requirement?

- A. Create a client VPN endpoint and configure the laptops to use an AWS client VPN to connect to the VPC over the internet.
- B. Create a new public virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX public virtual interface.
- C. Create a new Site-to-Site VPN that connects to the VPC over the internet.
- D. Create a new private virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX private virtual interface.

Commented [LC171]: You need a public virtual interface, check ref.

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html

D can not be correct due to this reason as per Tutorials Dojo: it is incorrect because you must use a public virtual interface for your AWS Direct Connect (DX) connection and not a private one. You won't be able to establish an encrypted VPN along with your DX connection if you create a private virtual interface."

Question #535

A business wants to launch a new application on five Amazon EC2 instances in a single AWS Region. The program needs high-speed, low-latency network connections between all of the Amazon EC2 instances on which it will execute. The application is not required to be fault tolerant.

Which solution will satisfy these criteria?

- A. Launch five new EC2 instances into a cluster placement group. Ensure that the EC2 instance type supports enhanced networking.
- B. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance.
- C. Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking.
- D. Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance.

Commented [LC172]: Answer is A. This question has two parts: in the first it talks about "needs high-speed, low-latency network connections between all of the Amazon EC2 instances" and in the second part it talks about "not required to be fault tolerant". Hence, the option A is best suited on this scenario.

Question #536

True or False: "In the context of Amazon ElastiCache, connecting to the cluster configuration endpoint is identical to connecting directly to an individual cache node from the application's perspective."

- 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.

Commented [LC173]: B is correct

Ref:
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Endpoints.html
https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/Endpoints.html

Question #537

An organization's IT operations team consists of four individuals who are responsible for managing the AWS infrastructure. The business want to configure the system in such a way that each user has the ability to launch and control an instance in a zone that the other user cannot alter.

Which of the following alternatives is the best way to configure this?

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

Commented [LC174]:

Question #538

You're developing a solution for connecting on-premises infrastructure to an Amazon VPC. Your on-premises servers will communicate with your VPC instances. You'll be creating IPSec tunnels over the Internet. You will use VPN gateways and AWS-supported customer gateways to terminate the IPSec tunnels.

Which of the following would you accomplish by constructing an IPSec tunnel in the manner described above? (Select 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

Commented [LC175]: My answer would be C, D, E, F.

For A, End to end protection means the secure tunnel has to be established between your EC2 instance and the on-perm machine. By establishing a VPN tunnel between VPC and your on-perm gateway does not achieve that, the traffic **before entering** and **after exiting** the VPN tunnel will not be encrypted.

For B, Same as A

For C, As explained in A, this is what you can achieve by established a VPN tunnel between the two gateway. (encryption only happen between the two VPN end point which protect the data when it travel on the internet)

For D, same as C

For E, when establishing the VPN tunnel, the two gateway will authenticate each other prior to form the VPN tunnel.

For F, same as C

Commented [LC176]:

Commented [LC177]:

Commented [LC178]:

Question #539

A business uses AWS to host an internal application that is used to monitor and process shipments at the company's warehouse. Currently, when the system gets an order, it sends the necessary information to the personnel to process the shipment. Once the product has been dispatched, the staff will respond to the email and mark the order as shipped.

The corporation want to phase out email in the application in favor of a serverless architecture.

Which architectural solution satisfies these criteria?

- A. Use AWS Batch to configure the different tasks required to ship a package. Have AWS Batch trigger an AWS Lambda function that creates and prints a shipping label. Once that label is scanned, as it leaves the warehouse, have another Lambda function move the process to the next step in the AWS Batch job.
- B. When a new order is created, store the order information in Amazon SQS. Have AWS Lambda check the queue every 5 minutes and process any needed work. When an order needs to be shipped, have Lambda print the label in the warehouse. Once the label has been scanned, as it leaves the warehouse, have an Amazon EC2 instance update Amazon SQS.
- C. Update the application to store new order information in Amazon DynamoDB. When a new order is created, trigger an AWS Step Functions workflow, mark the orders as "in progress", and print a package label to the warehouse. Once the label has been scanned and fulfilled, the application will trigger an AWS Lambda function that will mark the order as shipped and complete the workflow.
- D. Store new order information in Amazon EFS. Have instances pull the new information from the NFS and send that information to printers in the warehouse. Once the label has been scanned, as it leaves the warehouse, have Amazon API Gateway call the instances to remove the order information from Amazon EFS.

Commented [LC179]: Typical DynamoDB and AWS Step Functions usage.

Question #540

From an on-premises data center to AWS, a firm is transferring its marketing website and content management system. The organization wants to deploy the AWS application in a VPC using Amazon EC2 instances for web servers and an Amazon RDS instance for the database.
The firm maintains a runbook document that details the procedure of installing the on-premises system. The corporation wishes to build the AWS system on the basis of the procedures detailed in the runbook document. The runbook document details the server's operating systems, network settings, website, and content management system software installation and setup. Following the transfer, the organization wants to be able to make fast adjustments to take advantage of further AWS functionalities.

How can I install and automate the application and environment on 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.

Commented [LC180]: D
A: This is not automated.
B: This cannot be easily re-used for future.
C: The runbook is still considered manual configuration.

Only D is fully automated.

Question #541

Your application is not highly available, and your on-premises server is unable to reach the mount target due to the mount target's Availability Zone (AZ) being unavailable.

Which of the following is the suggested course of action?

- 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.

Commented [LC181]: 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.

Reference:
https://docs.aws.amazon.com/efs/latest/ug/performance-onpremises.html

Question #542 (EXAM)

A business wishes to transfer an application from VMware Infrastructure running in an on-premises data center to Amazon EC2. During the migration, a solutions architect must retain the software and configuration settings.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows File Server. Use the SMB share to host the VMware data store. Use VM Import/Export to move the VMs to Amazon EC2.
- B. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
- C. Configure AWS Storage Gateway for files service to export a Common Internet File System (CIFS) share. Create a backup copy to the shared folder. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- D. Create a managed-instance activation for a hybrid environment in AWS Systems Manager. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI. Launch an EC2 instance that is based on the AMI.

Commented [LC182]: B
- Export an OVF Template
- Create / use an Amazon S3 bucket for storing the exported images. The bucket must be in the Region where you want to import your VMs.
- Create an IAM role named vmimport.
- You'll use AWS CLI to run the import commands.

https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html

Question #543

A business is arranging a massive event to launch a special deal. AWS hosts the company's website, which is backed up by an Amazon RDS for PostgreSQL database instance. The website contains information about the offer and a sign-up page that captures user information and preferences. Management anticipates huge and unexpected quantities of traffic on a recurring basis, resulting in many database writes. A solutions architect must provide a solution that does not alter the underlying data architecture and prevents submissions from being discarded prior to being committed to the database.

Which solution satisfies these criteria?

- A. Immediately before the event, scale up the existing DB instance to meet the anticipated demand. Then scale down after the event.
- B. Use Amazon SQS to decouple the application and database layers. Configure an AWS Lambda function to write items from the queue into the database.
- C. Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling.
- D. Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance.

Commented [LC183]: B is correct. Remember with least amount of changes and unpredictable spike in volume it's better to go with a decoupled arch such as SQS.

Question #544

How can in-memory caching increase application speed with 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.

Commented [LC184]: 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.
Reference:
http://aws.amazon.com/elasticache/faqs/#g4

Question #545

A user has constructed a virtual private cloud (VPC) with a public subnet. The user has terminated all instances that were associated with the subnet.

Which of the following assertions is true in this scenario?

- A. The subnet to which the instances were launched with will be deleted
- B. When the user launches a new instance it cannot use the same subnet
- C. The user cannot delete the VPC since the subnet is not deleted
- D. Secondary network interfaces attached to the terminated instances may persist.

Commented [LC185]: D.
If interfaces created using aws-cli-> create-network-interface without option -> DeleteOnTermination, it will persist.

Also, before you can delete a VPC, you must terminate any instances that are running in the VPC. If you delete a VPC using the VPC console, it also deletes resources that are associated with the VPC, such as subnets, security groups, network ACLs, DHCP options sets, route tables, and Internet gateways.

Question #546

You've been engaged to improve a very big e-commerce site's overall security posture. They have a well-architected multi-tier application operating in a VPC, with ELBs in front of both the browser and application tiers, with static assets delivered straight from S3. They are storing dynamic data in a mix of RDS and DynamoDB and then archiving it nightly onto S3 for further processing using EMR. They are worried because they discovered suspicious log entries and suspect an effort at illegal entry.

Which strategy offers the most cost-effective and scalable defense against this kind of attack?

- A. Recommend that they lease space at a DirectConnect partner location and establish a 1G DirectConnect connection to their VPC they would then establish Internet connectivity into their space, filter the traffic in hardware Web Application Firewall (WAF). And then pass the traffic through the DirectConnect connection into their application running in their VPC.
- B. Add previously identified hostile source IPs as an explicit INBOUND DENY NACL to the web tier subnet.
- C. Add a WAF tier by creating a new ELB and an AutoScaling group of EC2 Instances running a host-based WAF. They would redirect Route 53 to resolve to the new WAF tier ELB. The WAF tier would their pass the traffic to the 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.

Commented [LC186]:

Question #547

A business has an application that makes use of Amazon EC2 instances that are part of an Auto Scaling group. To test the application, the Quality Assurance (QA) staff must establish a huge number of temporary environments. At the moment, the application environments are created by the department's manager using an AWS CloudFormation template. The Manager launches the stack by using a role that has authority to utilize the CloudFormation, EC2, and Auto Scaling APIs. The Manager wants to enable testers to create their own environments but does not like to provide each user extensive capabilities.

Which configuration would accomplish these objectives?

- 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 templates 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 permission 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 environment with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role.

Commented [LC187]:

Question #548

A business is establishing an AWS landing zone and has engaged a Solutions Architect to develop a multi-account access strategy that will enable hundreds of users to access the AWS Console using their corporate credentials. The organization uses Microsoft Active Directory, and users will connect to AWS through an AWS Direct Connect connection. Additionally, the corporation desires federation with third-party services and suppliers, including bespoke apps.

Which option satisfies the criteria with the LEAST amount of administrative 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.

Commented [LC188]: B is the correct answer.

A. Forms authentication is used for login to ADFS directly, so not relevant to AWS.
B. LEAST amount of work to use on premise AD, SSO to use other third party.
C. Since SSO can only have one directory, you can not use it for both on premise AD and third party at same time.
D. Would work but far more overhead than B, since it need configure ADFS by adding third party, as well as federation on AWS side.

https://docs.aws.amazon.com/singlesignon/latest/userguide/connectonpremad.html

https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html

Question #549 (SKIP)

In terms of Identity and Access Management (IAM), whatever form of special account associated with your application enables your code to programmatically access Google services?

- A. Service account
- B. Simple Key
- C. OAuth
- D. Code account

Commented [LC189]: Not a AWS related question, I think it's GCP.

Question #550

A company had a security breach in which an Amazon S3 bucket containing sensitive data was made public. The company policy is to have no public S3 objects, and the Compliance team must be notified promptly if any are discovered.

How can the existence of a public S3 item be recognized, configured to generate alert notifications, and then resolved automatically? (Select two.)

- A. Turn on object-level logging for Amazon S3. Turn on Amazon S3 event notifications to notify by using an Amazon SNS topic when a PutObject API call is made with a public-read permission.
- B. Configure an Amazon CloudWatch Events rule that invokes an AWS Lambda function to secure the S3 bucket.
- C. Use the S3 bucket permissions for AWS Trusted Advisor and configure a CloudWatch event to notify by using Amazon SNS.
- D. Turn on object-level logging for Amazon S3. Configure a CloudWatch event to notify by using an SNS topic when a PutObject API call with public-read permission is detected in the AWS CloudTrail logs.
- E. Schedule a recursive Lambda function to regularly change all object permissions inside the S3 bucket.

Commented [LC190]: B and D are the correct answers. While D detects the condition using cloud watch events and SNS topic, B actually performs the remediation. Others are incorrect because they fall to do either of the 2 things required in the question.

Commented [LC191]:

Question #551

A system administrator is responsible for the administration of an application hosted on AWS. The application is deployed on Amazon EC2, and the user has setup ELB and Auto Scaling. In anticipation of future load growth, the user intends to start additional servers in advance so that they may be registered with ELB.

How does the user add these instances to the Auto Scaling configuration?

- 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

Commented [LC192]: 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.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-manual-scaling.html

Question #552

A business has deployed AWS Organizations. It has lately created a number of new accounts and want to restrict access to a subset of AWS services under these newly created accounts.

How MOST effectively can this be controlled?

- 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.

Commented [LC193]: B
A\C: Not efficient.
D: Would affect all accounts.

Question #553

ABC is divided into three distinct departments, each of which has its own AWS account. The human resources department has established a file sharing portal to which all current workers' data is posted. The administration department uploads information about employee presence in the office to a database stored in the VPC. The Finance department need access to data from the Human Resources department in order to determine the number of on-roll workers and compute compensation based on the number of days an employee is in the office.

How is ABC going to put up this scenario?

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

Commented [LC194]:

Commented [LC195]: D is the only one that is true as it is stated.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-custom-resources.html

These services are designed to complement each other. AWS Elastic Beanstalk provides an environment to easily deploy and run applications in the cloud. It is integrated with developer tools and provides a one-stop experience for you to manage the lifecycle of your applications. AWS CloudFormation is a convenient provisioning mechanism for a broad range of AWS resources. It supports the infrastructure needs of many different types of applications such as existing enterprise applications, legacy applications, applications built using a variety of AWS resources and container-based solutions (including those built using AWS Elastic Beanstalk). AWS CloudFormation supports Elastic Beanstalk application environments as one of the AWS resource types. This allows you, for example, to create and manage an AWS Elastic Beanstalk- hosted application along with an RDS database to store the application data. In addition to RDS instances, any other supported AWS resource can be added to the group as well.
Reference:
https://aws.amazon.com/cloudformation/faqs

Question #554

You're looking to create and operate some new apps on AWS, and you're aware that Elastic Beanstalk and CloudFormation can both be used to automate the deployment of a wide variety of AWS resources.

Which of the following assertions is TRUE when comparing Elastic Beanstalk to CloudFormation?

- A. AWS Elastic Beanstalk introduces two concepts: The template, a JSON or YAML-format, text- based file
- B. Elastic Beanstalk supports AWS CloudFormation application environments as one of the AWS resource types.
- C. Elastic Beanstalk automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. CloudFormation does not.
- D. You can design and script custom resources in CloudFormation.

Question #555

A business is pursuing a multi-account approach, but the management team is concerned that services such as DNS may become too complicated. The organization requires a solution that enables the sharing of private DNS amongst virtual private clouds (VPCs) under distinct accounts. The firm will have a total of around 50 accounts.

Which option would result in the LEAST complicated DNS architecture possible while ensuring 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.

Commented [LC196]: This is the answer, but you also need to associate for each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings enableDnsHostnames and enableDnsSupport to true.

Question #556

Company B is introducing a new mobile gaming application. To speed data collection, users will log into the game using their current social network account.
Company B want to record player information and score information straight from the mobile app to a DynamoDB database called Score Data. When a user saves their game, the progress data is saved to the S3 bucket named Game state.

Which strategy is the best for storing data in 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.

Commented [LC197]: Web Identity Federation is the right way to store data in DynamoDB & S3 using existing social identities.

Question #557

A user has built a virtual private cloud (VPC) that has two subnets: one public and one private. The user intends to do a patch update for the private subnet instances.

How are the private subnet instances connected to the internet?

- A. The private subnet can never connect to the internet
- B. Use NAT with an elastic IP
- C. Use the internet gateway with a private IP
- D. Allow outbound traffic in the security group for port 80 to allow internet updates

Commented [LC198]: A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. A user can create a subnet with VPC and launch instances inside that subnet. If the user has created two subnets (one private and one public), they would need a Network Address Translation (NAT) instance with the elastic IP address. This enables the instances in the private subnet to send requests to the internet (for example, to perform software updates).

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

Question #558

A business operates a restaurant review website. The website is a single-page application that uses Amazon S3 to store files and Amazon CloudFront to distribute them. Each day, the company receives several fraudulent postings that are manually removed.
The security team determined that the majority of fraudulent postings originate from bots using IP addresses with a poor reputation inside the same geographical area. The team must devise a method for preventing bots from accessing the website.

Which approach should be used by a solutions architect?

- A. Use AWS Firewall Manage to control the CloudFront distribution security settings. Create a geographical block rule and associate it with Firewall Manager.
- B. Associate an AWS WAF web ACL with the CloudFront distribution. Select the managed Amazon IP reputation rule group for the web ACL with a deny action.
- C. Use AWS Firewall Manager to control the CloudFront distribution security settings. Select the managed Amazon IP reputation rule group and associate it with Firewall Manager with a deny action.
- D. Associate an AWS WAF web ACL with the CloudFront distribution. Create a rule group for the web ACL with a geographical match statement with a deny action.

Commented [LC199]: B: WAF with CloudFront using WebACL with Amazon IP reputation List which:
IP reputation rule groups allow you to block requests based on their source. Choose one or more of these rule groups if you want to reduce your exposure to BOTS, traffic or exploitation attempts

D blocks the entire region only for excluding some IPs.

Question #559

A business has five physical data centers in strategic locations across the globe. Each data center is equipped with hundreds of physical servers that run a combination of Windows and Linux-based applications and database services. Additionally, each data center has a 10 Gbps AWS Direct Connect link to AWS through a company-approved VPN solution to guarantee safe data transmission. The company's current data centers must be shut down immediately and servers and applications migrated to AWS.

Which solution satisfies these criteria?

- A. Install the AWS Server Migration Service (AWS SMS) connector onto each physical machine. Use the AWS Management Console to select the servers from the server catalog, and start the replication. Once the replication is complete, launch the Amazon EC2 instances created by the service.
- B. Install the AWS DataSync agent onto each physical machine. Use the AWS Management Console to configure the destination to be an AMI, and start the replication. Once the replication is complete, launch the Amazon EC2 instances created by the service.
- C. Install the CloudEndure Migration agent onto each physical machine. Create a migration blueprint, and start the replication. Once the replication is complete, launch the Amazon EC2 instances in cutover mode.
- D. Install the AWS Application Discovery Service agent onto each physical machine. Use the AWS Migration Hub import option to start the replication. Once the replication is complete, launch the Amazon EC2 instances created by the service.

Commented [LC200]: SMS is meant for migration of Virtual machines to AWS whereas Cloud Endure can be used for Physical, Virtual or Cloud Server. Hence C is correct.
https://aws.amazon.com/blogs/architecture/field-notes-choosing-a-rehost-migration-tool-cloudendure-or-aws-sms/

The question is outdated. Now the recommended solution from AWS is Application Migration Service.

https://aws.amazon.com/application-migration-service/

Question #560

A business wishes to host its website on Amazon Web Services (AWS) utilizing serverless architecture design principles for international consumers. The firm has specified the following requirements:

⇨ The website should be mobile-friendly.
⇨ The website's latency should be as low as possible.
⇨ The website should be really accessible.
⇨ Users should be able to log in using social identity providers such as Google, Facebook, or Amazon.
⇨ There should be basic DDoS safeguards in place to defend against traffic surges.

How are the design specifications to be met?

- A. Use Amazon CloudFront with Amazon ECS for hosting the website. Use AWS Secrets Manager to 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 and 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 resources. Use Amazon Cognito to provide user management authentication functions. Use AWS Lambda to build an API.

Commented [LC201]: The question mentions protection against DDoS attack. You can setup WAF on API gateway but you cannot set WAF on EKS, ECS nor Lambda.

Question #561

Is it possible for a user to set a custom health check for 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

Commented [LC202]: 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.

Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/healthcheck.html

Question #562

Is Amazon Cognito required to utilize 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.

Commented [LC203]: It's not called Amazon Pinpoint.

You can initialize Amazon Mobile Analytics using AWS IAM accounts. AWS recommend using Amazon Cognito for security best practices.
Reference:
http://aws.amazon.com/mobileanalytics/faqs/

Question #563 (EXAM)

A scientific organization requires the processing of text and picture data stored in an Amazon S3 bucket. The data is gathered from numerous radar stations during a mission's live, time-critical phase. The data is uploaded by the radar stations to the source S3 bucket. The data is preceded with the identification number of the radar station.
In a second account, the business built a destination S3 bucket. To satisfy a compliance target, data must be transferred from the source S3 bucket to the destination S3 bucket. Replication is accomplished by using an S3 replication rule that covers all items in the source S3 bucket.
A single radar station has been recognized as having the most precise data. At this radar station, data replication must be completed within 30 minutes of the radar station uploading the items to the source S3 bucket.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Set up an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert if this status changes.
- B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert when the time exceeds the desired threshold.
- C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert if this status changes.
- D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data. Enable S3 Replication Time Control (S3 RTC). Monitor the maximum replication time to the destination. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger an alert when the time exceeds the desired threshold.

Commented [LC204]: https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-time-control.html

Question #564

You're configuring several EBS volumes for a client that has requested a RAID configuration (redundant array of inexpensive disks). AWS has various suggestions about RAID configurations.

Which RAID configuration is not recommended for use with Amazon EBS?

- A. RAID 1 only
- B. RAID 5 only
- C. RAID 5 and RAID 6
- D. RAID 0 only

Commented [LC205]: C - RAID 5 or 6 are not recommended.

Question #565

A business has created a mobile game. The game's backend is hosted on many virtual machines in an on-premises data center. The business logic is available through a REST API that includes a variety of services. Session data for players is saved in a common file storage location. Backend services make use of distinct API keys to provide throttling and to differentiate between real and test traffic.
The game's backend load changes throughout the day. The server capacity is insufficient at peak hours. Additionally, there are latency difficulties while retrieving player session data. Management has tasked a solutions architect with developing a cloud architecture capable of coping with the game's fluctuating traffic and providing low-latency data access. The API model should not be altered in any way.

Which solution satisfies these criteria?

- A. Implement the REST API using a Network Load Balancer (NLB). Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless.
- B. Implement the REST API using an Application Load Balancer (ALB). Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- C. Implement the REST API using Amazon API Gateway. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- D. Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Aurora Serverless.

Commented [LC206]: C. Api Gateway.

DynamoDB typical gaming use case.
https://aws.amazon.com/blogs/database/amazon-dynamodb-gaming-use-cases-and-design-patterns/

Question #566

Which of the following is true of an instance profile established through the console when an IAM role is created?

- 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.

Commented [LC207]: 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. Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html

Question #567

You have been tasked with the responsibility of creating a public website on AWS that meets the following criteria:
You want the database and application server to be hosted on an Amazon Virtual Private Cloud (VPC). You want the database to be able to connect to the Internet in order for it to be automatically patched to the latest version.
You do not want the database to accept any inbound traffic from the Internet.

Which options would be the greatest fit for your intended public website hosted on AWS? (Select two.)

- A. Set up both the public website and the database on a public subnet and block all incoming requests from the Internet with a Network Access Control List (NACL)
- B. Set up both the public website and the database on a public subnet, and block all incoming requests from the Internet with a security group which only allows access from the IP of the public website.
- C. Set up the public website on a public subnet and set up the database in a private subnet which connects to the Internet via a NAT instance.
- D. Set up both the public website and the database on a private subnet and block all incoming requests from the Internet with a Network Access Control List (NACL). Set up a Security group between the public website and the database which only allows access via port 80.

Commented [LC208]: Can't find the second answer for this question. I believe that putting a DB in a public subnet is wrong in any case.

Question #568

A developer of a mobile game is distributing game assets across two AWS Regions. Each Region's game assets are provided via a cluster of Amazon EC2 instances behind an Application Load Balancer (ALB). The business demands that game assets be retrieved from the nearest Region. If the nearest Region's game assets become unavailable, they should be retrieved from the other Region.

What actions should a solutions architect take to ensure that these criteria are met?

- A. Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.
- B. Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
- C. Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.
- D. Create an Amazon Route 53 health check for each ALB. Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

Commented [LC209]:

Question #569

A firm is utilizing AWS to host a Node.js-based web-facing production application. The Development team is in charge of immediately deploying new versions of their software to production. The application software is updated on a daily basis. The team need advice from a Solutions Architect to ensure that the software is deployed to the production fleet swiftly and with little interruption to service.

Which alternative satisfies these criteria?

- 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.

Commented [LC210]: "C"
It's possible to avoid this downtime by performing a blue/green deployment, where you deploy the new version to a separate environment, and then swap CNAMEs of the two environments to redirect traffic to the new version instantly.

Question #570

A firm is migrating a mission-critical, multi-tier application to Amazon Web Services. The architecture is composed of a client application running on a desktop and a server infrastructure. The server architecture is hosted on-premises in a data center that regularly fails to meet the application's 99.95 percent uptime SLA. A Solutions Architect must redesign the application in order to guarantee that it meets or exceeds the SLA.
A PostgreSQL database is used in the program, which is hosted on a single virtual machine. Load balancing is used to distribute the business logic and display layers over numerous virtual machines. Remote users report experiencing lengthy load times while using this latency-sensitive application.

Which of the following approaches will fulfill availability requirements with little modification to the program while increasing user experience and lowering 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.

Commented [LC211]: Answer "B" meets the requirements.

A: using containers, is a big change to app. Maintaining EC2 is a challenge and could affect SLA. B: using RDS, is auto maintenance with high SLA. using autoscaling on EC2 allow more availability/performance. Appstream is good virtual solution. C: lots of re-works. D: there is no DB, only Datawarehouse.

Question #571

A client has a 10 GB AWS Direct Connect connection to an AWS region where an Amazon Elastic Computer Cloud web application is hosted (EC2).
The program is dependent on an on-premises mainframe database that adheres to the BASE (Basic Available, Soft state, Eventual consistency) model of consistency rather than the ACID (Atomicity, Consistency, Isolation, Durability) model. The application is behaving badly as a result of the database's inability to manage the number of writes.

How can you most cost-effectively lessen the burden on your on-premises database resources?

- 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.

Commented [LC212]: B is the right answer.

Question #572

On a fleet of Amazon EC2 instances, a business runs an application. Low latency and random access to 100 GB of data are required by the application. The program must be capable of performing data access at a rate of up to 3.000 IOPS. A development team designed the EC2 launch template to construct a 100-GB Provisioned IOPS (PIOPS) Amazon EBS volume with a provisioned IOPS capacity of 3000. A Solutions Architect's primary responsibility is to reduce costs without sacrificing performance or durability.

Which course of action should be followed?

- A. Create an Amazon EFS file system with the performance mode set to Max I/O. Configure the EC2 operating system to mount the EFS file system.
- B. Create an Amazon EFS file system with the throughput mode set to Provisioned. Configure the EC2 operating system to mount the EFS file system.
- C. Update the EC2 launch template to allocate a new 1-TB EBS General Purpose SSO (gp2) volume.
- D. Update the EC2 launch template to exclude the PIOPS volume. Configure the application to use local instance storage.

Commented [LC213]: B is correct EFS file system with the throughput mode set to Provisioned

A: File system in the Max I/O mode can scale to higher levels of aggregate throughput and operations per second. However, this scaling is done with a tradeoff of slightly higher latencies for file metadata operations.

B: Use the Provisioned Throughput mode on the EFS volume to ensure that the application can reach the required IOPS.

C: Although this may look cheaper at first, creating several 1TB volumes for each EC2 instance entails higher costs. The Amazon EFS volume solution will be cheaper for sharing storage across all EC2 instances. Although you can use EBS Multi-Attach to attach EBS volumes to multiple EC2 instances, this is limited only to Provisioned IOPS SSD (io1 or io2) volumes that are attached to Nitro-based EC2 instances in the same Availability Zone.

D: Instance local instance storage is ephemeral which means that you will lose all data in the volume when you stop/start the instance. This is not recommended for this mission-critical application.

Question #573

A business intends to move to AWS. A solutions architect searches the fleet using AWS Application Discovery Service and identifies an Oracle data warehouse and multiple PostgreSQL databases.

Which combination of migration patterns results in the lowest licensing and operating costs? (Select two.)

- A. Lift and shift the Oracle data warehouse to Amazon EC2 using AWS DMS.
- B. Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS DMS.
- C. Lift and shift the PostgreSQL databases to Amazon EC2 using AWS DMS.
- D. Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS.
- E. Migrate the Oracle data warehouse to an Amazon EMR managed cluster using AWS DMS.

Commented [LC214]: B & D

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database-to-amazon-rds-for-postgresql.html

Commented [LC215]: D is also right.

Question #574

A solutions architect is doing a workload migration to AWS Fargate. The job can only be executed on a private subnet inside the VPC that is not directly connected to the application from the outside world. When the Fargate job is initiated, the following error occurs: CannotPullContainerError: API failure (500): Obtain https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request aborted before connection was established

What should the solutions architect do to rectify this situation?

- A. Ensure the task is set to ENABLED for the auto-assign public IP setting when launching the task.
- B. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the public subnet in the VPC to route requests to the internet.
- C. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the private subnet in the VPC to route requests to the internet.
- D. Ensure the network mode is set to bridge in the Fargate task definition.

Commented [LC216]: B.

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task_cannot_pull_image.html

Question #575

You have customized your Amazon Elastic File System's Network File System (NFS) client settings (EFS). It may take up to three seconds for an Amazon Elastic Compute Cloud (EC2) instance to detect a write action on a file system executed by another EC2 instance.

Which of the following activities should you take to resolve the issue of modified NFS settings causing write operation delays?

- 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.

Commented [LC217]: 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.

Reference:
http://docs.aws.amazon.com/efs/latest/ug/troubleshooting.html#custom-nfs-settings-write-delays

Question #576

A business has a legacy application that runs on on-premises servers. The organization want to acquire actionable insights from application logs in order to boost the application's dependability. The following requirements for the solution have been provided to a Solutions Architect:

⇨ Aggregate logs using AWS.
⇨ Automate log analysis for errors.
⇨ Notify the Operations team when errors go beyond a specified threshold.

Which solution satisfies the specifications?

- A. Install Amazon Kinesis Agent on servers, send logs to Amazon Kinesis Data Streams and use Amazon Kinesis Data Analytics to identify errors, create an Amazon CloudWatch alarm to notify the Operations team of errors
- B. Install an AWS X-Ray agent on servers, send logs to AWS Lambda and analyze them to identify errors, use Amazon CloudWatch Events to notify the Operations team of errors.
- C. Install Logstash on servers, send logs to Amazon S3 and use Amazon Athena to identify errors, use sendmail to notify the Operations team of errors.
- D. Install the Amazon CloudWatch agent on servers, send logs to Amazon CloudWatch Logs and use metric filters to identify errors, create a CloudWatch alarm to notify the Operations team of errors.

Commented [LC218]: D
A: Amazon Kinesis Data Analytics used for data analytics.
B: Cannot be implemented on premise.
C: Athena is servers SQL based query system. Should use SNS instead of sendmail.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-premise.html

Question #577

Your firm just expanded its datacenter into an Amazon Web Services virtual private cloud (VPC) in order to increase burst computing capacity as required. Members of your Network Operations Center must have access to the AWS Management Console and the ability to manage Amazon EC2 instances as required. You do not want to establish new IAM users for each member of the NOC and need them to login in to the AWS Management Console repeatedly.

Which of the following options best meets the requirements of 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.

Commented [LC219]: C looks correct.

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

This specific use of SAML differs from the more general one illustrated at About SAML 2.0-based federation because this workflow opens the AWS Management Console on behalf of the user. This requires the use of the AWS SSO endpoint instead of directly calling the AssumeRoleWithSAML API. The endpoint calls the API for the user and returns a URL that automatically redirects the user's browser to the AWS Management Console.

Question #578

Recently, a company expanded via acquisitions. Two of the acquired businesses have the same IP CIDR range. There is a new short-term need that AnyCompany A (VPC-A) be able to interact with a server in AnyCompany B that has the IP address 10.0.0.77. (VPC-B). Additionally, AnyCompany A must communicate with all of the resources in AnyCompany C. (VPC-C). The Network team has established the VPC peer connections, but is experiencing communication difficulties between VPC-A and VPC-B. The team feels that the routing tables in the VPCs are inaccurate after an analysis.

Which setup will enable AnyCompany A to interact with AnyCompany C in addition to AnyCompany B's database?

- 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) on 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 (10.0.0.77/32) 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.

Commented [LC220]: D will work, /32 will be prioritized (Routing prioritize smaller cider). However, it will not be perfect, A wont able to communicate with 10.0.0.77 in VPC-C, because it will always be routed to B for that destination IP. But it is "short-term requirement " in this question, so the solution is acceptable.

Question #579

A business makes advantage of AWS Organizations. The business operates via an organization with a central management account. The organization intends to create many Amazon Web Services accounts for various departments. Each department account must be a member of the organization of the business.

According to compliance rules, each account must have a single VPC. Additionally, each VPC's network security setup must be identical, including fully configured subnets, gateways, network ACLs, and security groups.
The organization wishes for this security configuration to be deployed automatically whenever a new department account is established. The organization want to use the central management account for all security activities, however the central management account should be devoid of any security configuration.

Which technique satisfies these objectives with the MINIMUM amount of configuration?

- A. Create an OU within the company's organization. Add department accounts to the OU. From the central management account, create an AWS CloudFormation template that includes the VPC and the network security configurations. Create a CloudFormation stack set by using this template file with automated deployment enabled. Apply the CloudFormation stack set to the OU.
- B. Create a new organization with the central management account. Invite all AWS department accounts into the new organization. From the central management account, create an AWS CloudFormation template that includes the VPC and the network security configurations. Create a CloudFormation stack that is based on this template. Apply the CloudFormation stack to the newly created organization.
- C. Invite department accounts to the company's organization. From the central management account, create an AWS CloudFormation template that includes the VPC and the network security configurations. Create an AWS CodePipeline pipeline that will deploy the network security setup to the newly created account. Specify the creation of an account as an event hook. Apply the event hook to the pipeline.
- D. Invite department accounts to the company's organization. From the central management account, create an AWS CloudFormation template that includes the VPC and the network security configurations. Create an AWS Lambda function that will deploy the VPC and the network security setup to the newly created account. Create an event that watches for account creation. Configure the event to invoke the pipeline.

Commented [LC221]: https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-aws-organization/

Question #580

A solutions architect is debugging an Amazon EC2 instance-based application. The EC2 instances are managed as part of an Auto Scaling group. The application requires access to user data stored in a fixed-capacity Amazon DynamoDB database.

To accommodate the additional demand, the solutions architect recently raised the Auto Scaling group's maximum size. Now, when many instances are launched concurrently, some application components are throttled when they scan the DynamoDB database. The Auto Scaling group kills failed instances and creates new ones until all applications are operational.

A solutions architect must build a solution that resolves the throttling problem in the MOST cost-effective way possible.

Which solution will satisfy these criteria?

- A. Double the provisioned read capacity of the DynamoDB table.
- B. Duplicate the DynamoDB table. Configure the running copy of the application to select at random which table it access.
- C. Set the DynamoDB table to on-demand mode.
- D. Add DynamoDB Accelerator (DAX) to the table.

Commented [LC222]: C is the right answer.

Question #581

Is an AWS Direct Connect site capable of connecting to both Amazon Web Services in the region with which it is linked and to Amazon Web Services in other US regions?

- A. No, it provides access only to the region it is associated with.
- B. No, it provides access only to the US regions other than the region it is associated with.
- C. Yes, it provides access.
- D. Yes, it provides access but only when there's just one Availability Zone in the region.

Commented [LC223]: 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 (in case of a Direct Connect in a US region). for e.g., you can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US).

Question #582

By default, an EC2 instance performing source/destination checks is deployed on a private VPC subnet. All security, network access control, and routing definitions are established correctly. The launch of a custom NAT instance occurs.

Which of the following must be accomplished in order for the custom NAT instance to function properly? (Select Three)

- 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.

Commented [LC224]: 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.

Commented [LC225]:

Commented [LC226]:

Question #583

A firm is developing a pipeline for collecting sensor data in which thousands of sensors send data to an Amazon Simple Queue Service (Amazon SQS) queue on a minutely basis. The queue is handled by an AWS Lambda function that parses the sensor input and extracts a standard set of metrics. The business wishes to transmit the data to Amazon CloudWatch. Individual and aggregate sensor metrics should be viewable, as well as interactive querying of sensor log data through CloudWatch Logs Insights.

Which approach is the MOST cost-effective in terms of meeting these requirements?

- A. Write the processed data to CloudWatch Logs in the CloudWatch embedded metric format.
- B. Write the processed data to CloudWatch Logs. Then write the data to CloudWatch by using the PutMetricData API call.
- C. Write the processed data to CloudWatch Logs in a structured format. Create a CloudWatch metric filter to parse the logs and publish the metrics to CloudWatch with dimensions to uniquely identify a sensor.
- D. Configure the CloudWatch Logs agent for AWS Lambda. Output the metrics for each sensor in statsd format with tags to uniquely identify a sensor. Write the processed data to CloudWatch Logs.

Commented [LC227]: A is right

The CloudWatch embedded metric format is a JSON specification used to instruct CloudWatch Logs to automatically extract metric values embedded in structured log events. You can use CloudWatch to graph and create alarms on the extracted metric values.

https://aws.amazon.com/about-aws/whats-new/2019/11/amazon-cloudwatch-launches-embedded-metric-format/

Question #584

A user has created an Amazon Elastic Compute Cloud (EC2) instance in the us-east-1a zone. The user has chosen to monitor the instance in detail. The user is attempting to get data from CloudWatch using a command-line interface.

Which of the CloudWatch endpoint URLs listed below should the user use?

- A. monitoring.us-east-1a.amazonaws.com
- B. cloudwatch.us-east-1a.amazonaws.com
- C. monitoring.us-east-1.amazonaws.com
- D. monitoring.us-east-1-a.amazonaws.com

Commented [LC228]: Answer is C: https://docs.aws.amazon.com/general/latest/gr/cw_region.html

Question #585

A business maintains a Windows Server server on a public subnet that is configured to enable a team of administrators to connect through RDP and resolve problems with computers on a private subnet. Outside of regular maintenance windows, the host must be accessible at all times and must get the latest operating system upgrades within three days of release.

How should the host be managed with the LEAST amount of administrative work possible?

- 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 Chief 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.

Commented [LC229]: Answer: C

A - incorrect - Reason being the use of a "custom AMI" (won't work) and if it did, would lead to administrative overhead. "AMIs that aren't managed by Elastic Beanstalk aren't supported for Windows Server-based Elastic Beanstalk platforms." - a community Windows AMI cannot be used. Some additional info - single instance implies an ASG with a min/max of 1 (no diff to C). Single instance EC2 is deployed with a [public] Elastic IP address - only one that implies a public address.

B - incorrect - Updates running every 3 days doesn't mean an update is applied 3 days after release. It could be deployed 1 day after release if the next update cycle falls on that day. Also, Workspaces deploys Windows 10 desktop "experience" instances (1-to-1 mapping of user to host/instance) - we want a Bastion host that serves multiple users sessions simultaneously - not possible without BYOL and a physical host in AWS (complicated). Note: using WAM for hardening is possible, but requires a custom package created from a build & capture EC2 instance - fair bit of administrative overhead. WAM takes a snapshot before/after changes applied to the capture machine, and packges the deltas which can be pushed to the Workspace instance.

C - correct - technically feasible - may require a wrapper to manage termination policies to prevent ASG cycling the EC2 instance if the health check fails whilst updating/rebooting. Between A and C, its the only viable solution

D - incorrect - Upgrade Operating System stack is applicable to Linux only. Not Windows.
(ref for A - https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.customenv.html)

Question #586

A major corporation expanded its reliance on AWS in an unmanaged manner over time. As a result, they maintain a large number of separate AWS accounts across various business divisions, projects, and environments. The organization established a Cloud Center of Excellence to manage all elements of the AWS Cloud, including their AWS accounts.

Which of the following should the Cloud Center of Excellence team accomplish FIRST to concentrate their requirements? (Select two.)

- A. Control all AWS account root user credentials. Assign AWS IAM users in the account of each user who needs to access AWS resources. Follow the policy of least privilege in assigning permissions to each user.
- B. Tag all AWS resources with details about the business unit, project, and environment. Send all AWS Cost and Usage reports to a central Amazon S3 bucket, and use tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.
- C. Use the AWS Marketplace to choose and deploy a Cost Management tool. Tag all AWS resources with details about the business unit, project, and environment. Send all AWS Cost and Usage reports for the AWS accounts to this tool for analysis.
- D. Set up AWS Organizations. Enable consolidated billing, and link all existing AWS accounts to a master billing account. Tag all AWS resources with details about the business unit, project and environment. Analyze Cost and Usage reports using tools such as Amazon Athena and Amazon QuickSight, to collect billing details by business unit.
- E. Using a master AWS account, create IAM users within the master account. Define IAM roles in the other AWS accounts, which cover each of the required functions in the account. Follow the policy of least privilege in assigning permissions to each role, then enable the IAM users to assume the roles that they need to use.

Commented [LC230]: That's a typical Landing Zone Template

Commented [LC231]:

Question #587

The CISO of a big corporation with many IT departments, each with their own AWS account, desires a centralized location for managing AWS permissions for users and synchronizing users authentication credentials with the company's current on-premises solution.

Which solution will fulfill the standards of the CISO?

- A. Define AWS IAM roles based on the functional responsibilities of the users in a central account. Create a SAML-based identity management provider. Map users in the on-premises groups to IAM roles. Establish trust relationships between the other accounts and the central account.
- B. Deploy a common set of AWS IAM users, groups, roles, and policies in all of the AWS accounts using AWS Organizations. Implement federation between the on-premises identity provider and the AWS accounts.
- C. Use AWS Organizations in a centralized account to define service control policies (SCPs). Create a SAML-based identity management provider in each account and map users in the on-premises groups to AWS IAM roles.
- D. Perform a thorough analysis of the user base and create AWS IAM users accounts that have the necessary permissions. Set up a process to provision and deprovision accounts based on data in the on-premises solution.

Commented [LC232]: C
To help you manage federation for multiple AWS accounts centrally, you can use AWS Single Sign-On to manage SSO access for all of your accounts in AWS Organizations.
https://aws.amazon.com/identity/federation/

A: The fact that the answer did not explain how "trust relationships" are created means I would avoid this answer if there is a better answer. In this case C. You will also need to use a lot of assume roles in each and every account which can be tedious. This was what it used to be before AWS Organization was launched.

B: Accounts are not centralized. ("one central place")

D: There is no federation.

Question #588

Which of the following AWS services may be used to establish alerts that will be triggered based on the success, failure, or delay of an operation in AWS Data Pipeline?

- A. Amazon SES
- B. Amazon CodeDeploy
- C. Amazon SNS
- D. Amazon SQS

Commented [LC233]: 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.
Reference:
https://aws.amazon.com/datapipeline/faqs/

Question #589

A business has the following Amazon EC2 deployment 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 breaks, customers claim that their requests are processed very slowly. A Solutions Architect must make architectural adjustments to ensure the system's dependability is maximized. Costs must be kept to a minimum.

What recommendations should the Solutions Architect make?

- 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

Commented [LC234]: C.

The requirement states cost must be reduced.
A - while lambda may reduce cost in run, no details on effort required in changing application & feasibility.
B- The question mention slowness in processing jobs which indicates load. Again no mention of application using L4/L7.
C. Auto scaling can reduce cost and improve reliability.
D. Increasing size means more congestion when a EC2 fails.

Question #590

On Amazon EC2, a corporation now operates a secure application that accepts files from on-premises locations through AWS Direct Connect, processes them, and uploads them to a single Amazon S3 bucket. The program encrypts data in transit to Amazon S3 using HTTPS, and data at rest using S3 server-side encryption.

Which of the following modifications should the Solutions Architect propose to increase the security of this system without impairing its 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.

Commented [LC235]: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

When a request comes from a VPC endpoint the ip is under Source:vpce and not Source:ip so B can't be true.

A, C ruled out.

Question #591

Which stage of the AWS Direct Connect process should the user do in order to ascertain the needed port speed?

- A. Complete the Cross Connect
- B. Verify Your Virtual Interface
- C. Download Router Configuration
- D. Submit AWS Direct Connect Connection Request

Commented [LC236]: To submit an AWS Direct Connect connection request, you need to provide the following information:
Your contact information.
The AWS Direct Connect Location to connect to.
Details of AWS Direct Connect partner if you use the AWS Partner Network (APN) service. The port speed you require, either 1 Gbps or 10 Gbps.
Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#ConnectionRequest

Question #592

A security team uncovered during an audit that a development team was embedding IAM user secret access keys in their code and then pushing it to an AWS CodeCommit repository. The security team wants to detect and remedy occurrences of this security vulnerability automatically.

Which solution will automatically safeguard the credentials in the suitable manner?

- A. Run a script nightly using AWS Systems Manager Run Command to search for credentials on the development instances. If found, use AWS Secrets Manager to rotate the credentials.
- B. Use a scheduled AWS Lambda function to download and scan the application code from CodeCommit. If credentials are found, generate new credentials and store them in AWS KMS.
- C. Configure Amazon Macie to scan for credentials in CodeCommit repositories. If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user.
- D. Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.

Commented [LC237]: https://docs.aws.amazon.com/codecommit/latest/userguide/data-protection.html

https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-notify-lambda.html

Macie is for S3. It's D.

Question #593

A business has an Amazon S3 data lake that must be accessible by hundreds of apps across several AWS accounts. According to the company's information security policy, the S3 bucket must not be accessible through the public internet and each application should have the bare minimal rights required to operate.
To achieve these criteria, a solutions architect intends to utilize an S3 access point that is confined to unique virtual private clouds (VPCs) for each application.

Which actions should the solutions architect perform in conjunction to implement this solution? (Select two.)

- A. Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point
- B. Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint
- C. Create a gateway endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
- D. Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
- E. Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket

Commented [LC238]: A, C.

https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/

https://aws.amazon.com/blogs/storage/setting-up-cross-account-amazon-s3-access-with-s3-access-points/ => Account A (The Data Owner). This is the account you create the Amazon S3 Access Point in

Commented [LC239]:

Question #594

A business is operating an application on many Amazon EC2 instances that are part of an Auto Scaling group and are protected by an Application Load Balancer. The application's demand changes throughout the day, and EC2 instances are often scaled in and out. Every 15 minutes, log files from the EC2 instances are moved to a central Amazon S3 bucket. The security team notices that log files have been deleted from many terminated EC2 instances.

Which series of activities will guarantee that log files from terminated EC2 instances are transferred to the central S3 bucket?

- A. Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to send ABANDON to the Auto Scaling group to prevent termination run the script to copy the log files, and terminate the instance using the AWS SDK.
- B. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group. Invoke an AWS Lambda function on the autoscaling:EC2_INSTANCE_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.
- C. Change the log delivery rate to every 5 minutes. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect EC2 instance termination. Invoke an AWS Lambda function from the EventBridge (CloudWatch Events) rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
- D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic. From the SNS notification call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance.

Commented [LC240]: SSM document is reliable way to copy the data from EC2 instance.

Question #595

_____ pricing represents a considerable discount on the standard price for DynamoDB provided throughput capacity.

- A. Discount Voucher
- B. Reserved Capacity
- C. Discount Service
- D. Reserved Point

Commented [LC241]: 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.
Reference:
http://aws.amazon.com/dynamodb/pricing/

Question #596

A gaming firm established a game leaderboard by deploying an Amazon RDS database in a Multi-AZ configuration. The number of users is increasing, and inquiries for individual player rankings are becoming more sluggish. The firm anticipates a spike in user activity for a forthcoming update and want to improve the design for scalability and performance.

Which solution will satisfy these criteria?

- A. Migrate the database to Amazon DynamoDB. Store the leaderboard data in two different tables. Use Apache HiveQL JOIN statements to build the leaderboard.
- B. Keep the leaderboard data in the RDS DB instance. Provision a Multi-AZ deployment of an Amazon ElastiCache for Redis cluster.
- C. Stream the leaderboard data by using Amazon Kinesis Data Firehose with an Amazon S3 bucket as the destination. Query the S3 bucket by using Amazon Athena for the leaderboard.
- D. Add a read-only replica to the RDS DB instance. Add an RDS Proxy database proxy.

Commented [LC242]: D. RDS Proxy makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections. Using RDS Proxy, you can handle unpredictable surges in database traffic that otherwise might cause issues due to oversubscribing connections or creating new connections at a fast rate.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html

Question #597

A user is operating a mission-critical batch process that runs for one hour and fifty minutes each day at a predetermined time.

Which of the following is the appropriate instance type and pricing model in this example if the user does the same job continuously throughout the year?

- A. Instance store backed instance with spot instance pricing.
- B. EBS backed instance with standard reserved upfront instance pricing.
- C. EBS backed scheduled reserved instance with partial instance pricing.
- D. EBS backed instance with on-demand instance pricing.

Commented [LC243]: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

For Amazon Web Services, the reserved instance (standard or convertible) helps the user save money if the user is going to run the same instance for a longer period. Generally, if the user uses the instances around 30-40% of the year annually it is recommended to use RI. Here as the instance runs only for 1 hour 50 minutes daily, or less than 8 percent of the year, it is not recommended to have RI as it will be costlier. At its highest potential savings, you are still paying 25 percent of an annual cost for a reserved instance you are you using less than 2 hours a day, (or less than 8 percent of each year) you are not saving money. Even a scheduled reserved instance has a key limitation, which is that it cannot be stopped or rebooted, only manually terminated with a possibility that it could be restarted. You would have to terminate and restart it within the 1 hour 50-minute window, otherwise you would need to wait until the next day. For a critical daily process, this is likely not an option. Spot Instances are not ideal because the process is critical, and must run for a fixed length of time at a fixed time of day. Spot instances would stop and start based on fluctuations in instance pricing, leaving this process potentially unfinished. The user should use on-demand with EBS in this case. While it has the highest cost, it also has the greatest flexibility to ensure that a critical process like this is always completed.

Question #598

A business has hired a Solutions Architect to create a secure content management system that can be accessed through API calls from external customer apps.
The organization demands that a client administrator be able to make API calls and, if necessary, roll back modifications to existing files provided to the content management system.

Which deployment strategy is the MOST SECURE and satisfies all solution requirements?

- A. Use Amazon S3 for object storage with versioning and bucket access logging enabled, and an IAM role and access policy for each customer application. Encrypt objects using SSE-KMS. Develop the content management application to use a separate AWS KMS key for each customer.
- B. Use Amazon WorkDocs for object storage. Leverage WorkDocs encryption, user access management, and version control. Use AWS CloudTrail to log all SDK actions and create reports of hourly access by using the Amazon CloudWatch dashboard. Enable a revert function in the SDK based on a static Amazon S3 webpage that shows the output of the CloudWatch dashboard.
- C. Use Amazon EFS for object storage, using encryption at rest for the Amazon EFS volume and a customer managed key stored in AWS KMS. Use IAM roles and Amazon EFS access policies to specify separate encryption keys for each customer application. Deploy the content management application to store all new versions as new files in Amazon EFS and use a control API to revert a specific file to a previous version.
- D. Use Amazon S3 for object storage with versioning and enable S3 bucket access logging. Use an IAM role and access policy for each customer application. Encrypt objects using client-side encryption, and distribute an encryption key to all customers when accessing the content management application.

Commented [LC244]: The correct answer is A.

C is not a best practice.

D is incorrect since in Customer managed CMK, the customer is expected to provide the encryption key and not be supplied one from AWS.

B is a bit vague when it comes to the last sentence around enabling revert function based on the static web page hosted on S3 that contains CloudWatch logs accumulated from CloudTrail.

Question #599

A business intends to build a secure, scalable application using AWS VPC and ELB. The organization now has two instances operating, each with an ENI in addition to a principal network interface. Both the main network interface and the auxiliary ENI are equipped with an elastic IP.

If those instances are registered with ELB and the organization wishes for ELB to deliver data to a specific instance's EIP, how can this be accomplished?

- 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.

Commented [LC245]: 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

Questions 600-699

Question #600

A mobile gaming application transmits data to Amazon Kinesis Data Streams on a continual basis. AWS Lambda analyses the data stream records and publishes them to an Amazon DynamoDB database. The DynamoDB table has an enabled auto scaling strategy with a target usage of 70%. Each day, for several minutes at the beginning and end of the day, there is a traffic surge that often surpasses five times the average load. The corporation becomes aware of the GetRecords. For many minutes, the IteratorAgeMilliseconds metric of the Kinesis data stream surges to over a minute. During certain moments, the AWS Lambda function logs ProvisionedThroughputExceededException messages to Amazon CloudWatch Logs and redirects some records to the dead letter queue.
On the gaming application, the Kinesis producer throws no exceptions.

What changes should the business do to address this issue?

- A. Use Application Auto Scaling to set a scaling schedule to scale out write capacity on the DynamoDB table during predictable load spikes.
- B. Use Amazon CloudWatch Events to monitor the dead letter queue and invoke a Lambda function to automatically retry failed records.
- C. Reduce the DynamoDB table auto scaling policy's target utilization to 20% to more quickly respond to load spikes.
- D. Increase the number of shards in the Kinesis data stream to increase throughput capacity.

Commented [LC246]: Option A.

This is a case of piling records for processing. Kinesis GetRecords.IteratorAgeMilliseconds increasing indicates that records are being processed slowly and this higlights the risk of records expiring.

ProvisionedThroughputExceededException indicates request rate is too high. AWS API Doc says - Reduce the frequency of requests and use exponential backoff so they can be processed. To ensure the records are processed quickly during surge times which is known ahead write capacity should be increased.

Related information - When Kinesis Producer is writing to KDS - the capacity is determined by the number of shards (provisioned mode where the load is known). AWS supports on-demand mode where the shards are scaled up/down. Each shard for writing is able to handle 1MB/Sec. So, if we need to increase write we need to increase the shards. This is not relevant in our case as the data is getting written and Lambda is able to read from the shards.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

Question #601

To assist with service deployment, a development team has built a number of AWS CloudFormation templates. They developed a framework for a network/virtual private cloud (VPC) stack, a database stack, a bastion host stack, and a stack specifically for web applications. Each service requires the deployment of at least the following:
⇨ A network/Virtual Private Cloud stack
⇨ A host stack that serves as a bastion
⇨ A stack of web applications
Each template has a large number of input parameters, making it impossible to install the services independently using the AWS CloudFormation panel. Typically, the input parameters of one stack are the outputs of other stacks. For instance, the network stack's VPC ID, subnet IDs, and security groups may need to be utilized in the application or database stack.

Which activities will contribute to lowering both the operational load and the amount of parameters supplied into a service deployment? (Select 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.

Commented [LC247]: A&E. E requires few parameters and one action to launch a portfolio to deploy all products, where one product represents one service. Between A (CloudFormation console to deploy a service) vs D (Step function to deploy a service) I chose A because I didn't find Step function to be a standard practice to deploy a cloudformation stack unlike CodePipeline which is a standard way to test and deploy cloudformation stack via a codepipeline. However Option B and C fall short because they do not reduce the # of input parameters.

Commented [LC248]:

Question #602

A business is transferring its on-premises build artifact server to an Amazon Web Services (AWS) solution. The existing system is comprised of an Apache HTTP server that provides artifacts to clients inside the perimeter firewall's local network. The majority of artifact consumers are built-in automation scripts that download artifacts over anonymous HTTP, which the firm will be unable to adjust during the timeframe of its migration. The business chooses to migrate to Amazon S3 static website hosting. The artifact consumers will be transferred to Amazon EC2 instances inside a virtual private cloud's public and private subnets (VPC).

Which solution enables artifact consumers to download artifacts without altering the automated processes already in place?

- A. Create a NAT gateway within a public subnet of the VPC. Add a default route pointing to the NAT gateway into the route table associated with the subnets containing consumers. Configure the bucket policy to allow the s3:ListBucket and s3:GetObject actions using the condition IpAddress and the condition key aws:SourceIp matching the elastic IP address of the NAT gateway.
- B. Create a VPC endpoint and add it to the route table associated with subnets containing consumers. Configure the bucket policy to allow s3:ListBucket and s3:GetObject actions using the condition StringEquals and the condition key aws:sourceVpce matching the identification of the VPC endpoint.
- C. Create an IAM role and instance profile for Amazon EC2 and attach it to the instances that consume build artifacts. Configure the bucket policy to allow the s3:ListBucket and s3:GetObjects actions for the principal matching the IAM role created.
- D. Create a VPC endpoint and add it to the route table associated with subnets containing consumers. Configure the bucket policy to allow s3:ListBucket and s3:GetObject actions using the condition IpAddress and the condition key aws:SourceIp matching the VPC CIDR block.

Commented [LC249]: A wrong - "aws:SourceIp matching the elastic IP address of the NAT gateway" will not serve instances in public subnets
B OK - aws:sourceVpce
C wrong - no access to S3 from private subnets
D wrong - with Vpce instead of aws:SourceIp you have to use aws:VpcSourceIp

Question #603

A client of AWS is launching an application that utilizes an AutoScaling group of EC2 Instances.
According to the customer's security policy, any outbound connections from these instances to any other service inside the customer's Virtual Private Cloud must be authenticated using a unique x509 certificate including the instance's unique id.
Additionally, to be trusted for authentication, an x509 certificate must be created by the customer's key management service.

Which of the following setups meets these specifications?

- 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.

Commented [LC250]: Answer is C
A - seems to be wrong because if a single certificate is stored in S3, it would have a single key pair and a single signature which would be duplicated across all instances. Does not fulfill the instance-id uniqueness

B - similar issue of duplicate private key but more importantly, the first outbound request from the instance to the KMS (for certificate signing) will not be signed, which violates the policy

D - A new certificate is generated upon each instance spin-up. Without sending out a signing request (with the signature of the newly generated key-pair), how can the KMS send a valid signed certificate.

Question #604

A user is attempting to connect to an EC2 instance through the SSH port 10.20.30.40/32.

Which of the following is the most secure method of configuring the instance such that it 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

Commented [LC251]: 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.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

Question #605

A software business runs an application on Amazon Web Services (AWS) using resources spread across many AWS accounts and regions. The application is hosted on a cluster of Amazon EC2 instances in a virtual private cloud (VPC) in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a separate AWS account, a shared services VPC with an IPv4 CIDR block of 10.10.10.0/24 is placed in the us-east-2 Region. When a cloud engineer attempts to peer the application VPC with the shared services VPC using AWS CloudFormation, an error message shows a peering failure.

Which variables may have contributed to this error? (Select two.)

- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer accepter account does not have the correct permissions

Commented [LC252]: its A & E. Cloud engineer uses "AWS CloudFormation" to attempt to peer the application. https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-vpc-peering-error/

Commented [LC253]:

Question #606

A North American corporation with its headquarters on the East Coast is implementing a new web application in the us-east-1 Region using Amazon EC2. The application's scalability should be dynamic in order to satisfy user demand while maintaining resilience. Additionally, the application must support active-passive disaster recovery in the us-west-1 Region.

Which actions should a solutions architect take after the creation of a virtual private cloud in the us-east-1 region?

- A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
- B. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.
- C. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.
- D. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

Commented [LC254]: A, C ruled out, there is no need of connecting the two VPCs. D is ruled out because Route53 is a global service and does not have per-region records.

B is good.

Question #607

A company's recommendation service for video games has just gone popular. The firm is gaining new customers from all corners of the globe. The service's website is hosted on a collection of Amazon EC2 instances organized in an Auto Scaling group and protected by an Application Load Balancer (ALB). The website is composed of static content, with resources being loaded in accordance with the device type.
Recently, users claimed that the website's load time has risen. Administrators are reporting that the EC2 instances that host the service are experiencing significant demands.

Which specific activities should a solutions architect take in order to increase response times?

- A. Create separate Auto Scaling groups based on device types. Switch to Network Load Balancer (NLB). Use the User-Agent HTTP header in the NLB to route to a different set of EC2 instances.
- B. Move content to Amazon S3. Create an Amazon CloudFront distribution to serve content out of the S3 bucket. Use Lambda@Edge to load different resources based on the User-Agent HTTP header.
- C. Create a separate ALB for each device type. Create one Auto Scaling group behind each ALB. Use Amazon Route 53 to route to different ALBs depending on the User-Agent HTTP header.
- D. Move content to Amazon S3. Create an Amazon CloudFront distribution to serve content out of the S3 bucket. Use the User-Agent HTTP header to load different content.

Commented [LC255]: Totally agree on B.

Here's the exact fragment URL on that page to the code to redirect based on device type:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-vary-on-device-type

option B is a more sophisticated solution than option D, even if D is possible: "You can configure CloudFront to cache objects based on values in the User-Agent header, but we don't recommend it. The User-Agent header has many possible values, and caching based on those values would cause CloudFront to forward significantly more requests to your origin."
Ref: Same link shared in ref below
D is actually OK as the content to deliver depends only on the "device type". If more complicated criteria were involved, Lambda@Edge would be needed...

This is a bit tricky and any thoughts here are welcome.

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorCustomOrigin.html#request-custom-user-agent-header

Question #608 (EXAM)

A business is executing a workload on thousands of Amazon EC2 instances. The workload is operating on a virtual private cloud (VPC) that comprises many public and private subnets. The public subnets provide a route for 0.0.0.0/0 to an already-established internet gateway. Each private subnet has a route to an existing NAT gateway for 0.0.0.0/0.
A solutions architect is responsible for migrating a complete fleet of Amazon EC2 instances to IPv6. Private subnet EC2 instances must be inaccessible from the public internet.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway.
- B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for ::/0 to the NAT gateway.
- C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Create an egress-only internet gateway. Update the VPC route tables for all private subnets, and add a route for ::/0 to the egress-only internet gateway.
- D. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPv6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6-enabled NAT gateway.

Commented [LC256]: A - Incorrect - It will allow instances to be accessed from internet
B - Incorrect - NAT gateways are not supported for IPv6 traffic—use an outbound-only (egress-only) internet gateway instead.
C- Correct.
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html#vpc-migrate-ipv6-cidr
D: Incorrect - NAT gateways are not supported for IPv6 traffic—use an outbound-only (egress-only) internet gateway instead.

Question #609

A solutions architect must establish a reference architecture for a solution that consists of three tiers: web, application, and NoSQL data. The reference architecture must conform to the following criteria:
⇨ Within an AWS Region, there is a high level of availability.
⇨ Capable of failing over to another AWS Region in less than a minute for disaster recovery
⇨ Provide the most efficient solution possible while mitigating any negative influence on the user experience

Which combination of actions will satisfy these criteria? (Select three.)

- A. Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.
- B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.
- C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
- D. Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region. Have a script import the data into DynamoDB in a disaster recovery scenario.
- E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.
- F. Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.

Commented [LC257]: B,C,E is perfect answer.
The requirements can be achieved by using an Amazon DynamoDB database with a global table. DynamoDB is a NoSQL database so it fits the requirements. A global table also allows both reads and writes to occur in both Regions. For the web and application tiers Auto Scaling groups should be configured. Due to the 1-minute RTO these must be configured in an active/passive state. The best pricing model to lower price but ensure resources are available when needed is to use a combination of zonal reserved instances and on-demand instances.
To failover between the Regions, a Route 53 failover routing policy can be configured with a TTL configured on the record of 30 seconds. This will mean clients must resolve against Route 53 every 30 seconds to get the latest record. In a failover scenario the clients would be redirected to the secondary site if the primary site is unhealthy.

Commented [LC258]:

Commented [LC259]:

Question #610

A business has many Amazon EC2 instances linked to both public and private subnets inside a virtual private cloud (VPC) that is not connected to the corporate network. A security group connected with the EC2 instances enables the firm to access the instances using the Windows remote desktop protocol (RDP) via the internet. The security team has detected attempted connections from unidentified sources. The business wants to establish a more secure method of accessing its EC2 instances.

Which approach should be implemented by a solutions architect?

- A. Deploy a Linux bastion host on the corporate network that has access to all instances in the VPC.
- B. Deploy AWS Systems Manager Agent on the EC2 instances. Access the EC2 instances using Session Manager restricting access to users with permission.
- C. Deploy a Linux bastion host with an Elastic IP address in the public subnet. Allow access to the bastion host from 0.0.0.0/0.
- D. Establish a Site-to-Site VPN connecting the corporate network to the VPC. Update the security groups to allow access from the corporate network only.

Commented [LC260]:

Question #611

A user wants to arrange AutoScaling such that it scales up when the CPU usage exceeds 70% and down when the CPU utilization is less than 30%.

How can the user set AutoScaling to accommodate the aforementioned circumstance?

- 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

Commented [LC261]: 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.

Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/as-scale-based-on-demand.html

Question #612

You must be able to evaluate a customer's website clickstream data in order to do behavioral analysis. Your customer wants to know which sites and advertisements their consumer clicked on in order. This information will be utilized in real time to adjust the page layouts as users navigate the site in order to maximize stickiness and advertising click-through.

Which of the following options satisfies the criteria for captioning and analysis of 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.

Commented [LC262]: B.
Kinesis to support "data will be used in real time" requirement.

Question #613

You want to establish a mirror replica of your production environment in another area in order to facilitate catastrophe recovery.

Which of the following Amazon Web Services resources does not need replication in the second region? (Select two.)

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

Commented [LC263]:

Commented [LC264]:

Question #614

How do I migrate an EBS volume that is presently tied to an EC2 instance to a different Availability Zone?

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

Commented [LC265]: The EBS Volumes attached to the EC2 Instance will always have to remain in the same availability zone as the EC2 Instance. Possible reason to this is because of the fact that EBS Volumes are present outside of the host machine and instances have to be connected over the network, if the EBS Volumes are present outside the Availability Zone there can be potential latency issues and subsequent performance degradation.

What you can do in such scenario is, get the Snapshot of the EBS Volume (Snapshot sequentially captures the state of your EBS Volume and stores it in S3 Bucket (friendly reminder that it will cost you)) and post that you have two options , you can either create an EBS Volume from this snapshot in your desired Availability Zone or you can create an AMI from this snapshot in your desired Availability Zone and then go ahead and launch your EC2 instance from it.

Question #615

A provisioned IOPS volume must have a minimum size of __ GB:

- A. 20
- B. 10
- C. 50
- D. 1

Commented [LC266]: Outdated question. It's 4 GB

Question #616

Mike gets promoted to the position of Cloud Consultant at ABC.com. ABC has established the following VPCs in the US East Region:
A VPC with CIDR block 10.10.0.0/16 and a subnet with CIDR block 10.10.1.0/24. A VPC with CIDR block 10.40.0.0/16 and a subnet with CIDR block 10.40.1.0/24. A VPC with CIDR block 10.40.0.0/16 and a subnet with CIDR block 10.40.1.0/24.
ABC.com is attempting to create a network connection between two subnets, one with the CIDR block 10.10.1.0/24 and another with the CIDR block 10.40.1.0/24.
10.40.1.0/24 is a block.

Mike should offer which of the following options to ABC.com.

- A. Create 2 Virtual Private Gateways and configure one with each VPC.
- B. Create 2 Internet Gateways, and attach one to each VPC.
- C. Create a VPC Peering connection between both VPCs.
- D. Create one EC2 instance in each subnet, assign Elastic IPs to both instances, and configure a set up Site-to-Site VPN connection between both EC2 instances.

Commented [LC267]: A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. EC2 instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware.

Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

Question #617

An online corporation want to integrate an intrusion detection and prevention system into their deployed virtual private cloud (VPC). This platform should be scalable to thousands of instances inside the VPC.

How should they construct their solution in order to accomplish these objectives?

- A. Configure an instance with monitoring software and the elastic network interface (ENI) set to promiscuous mode packet sniffing to see 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.

Commented [LC268]: So, i googled and found this on a site:
B is the correct answer.

The key line of the question is "thousands of instances running in the VPC".

Option C does not confirm that the incoming traffic is passed through the IDS/IPS before reaching the host, which is one of the primary feature/requirements of any IDS/IPS. The traffic will need to pass through the IDS so that any vulnerability could be assessed. Moreover, in Option C, you can not expect to manage thousands and thousands of Servers through host-based routing.

Option A is invalid as promiscuous mode is not supported in AWS.

Option D does not meet the IPS requirement and moreover although it can perform IDS activities but again it is not a scalable solution.

SO, OPTION B is the correct ANSWER.

Question #618

A federal customer needs your assistance in establishing safe cryptographic key storage for some of their most sensitive data. You determine that AWS CloudHSM is the most appropriate service for this.
However, there seem to be a few prerequisites for this to occur, one of which is a security group that maintains access to specified ports.

Which of the following statements about the security groups is correct?

- A. A security group that has no ports open to your network.
- B. A security group that has only port 3389 (for RDP) open to your network.
- C. A security group that has only port 22 (for SSH) open to your network.
- D. A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network.

Commented [LC269]: AWS CloudHSM provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud.
AWS CloudHSM requires the following environment before an HSM appliance can be provisioned. A virtual private cloud (VPC) in the region where you want the
AWS CloudHSM service. One private subnet (a subnet with no Internet gateway) in the VPC. The HSM appliance is provisioned into this subnet.
One public subnet (a subnet with an Internet gateway attached). The control instances are attached to this subnet.
An AWS Identity and Access Management (IAM) role that delegates access to your AWS resources to AWS CloudHSM.
An EC2 instance, in the same VPC as the HSM appliance, that has the SafeNet client software installed. This instance is referred to as the control instance and is used to connect to and manage the HSM appliance.
A security group that has port 22 (for SSH) or port 3389 (for RDP) open to your network. This security group is attached to your control instances so you can access them remotely.

Question #619

On AWS, a business developed an ecommerce website utilizing a three-tier web architecture. The program is written in Java and is built on an Amazon CloudFront distribution, an Apache web server layer comprised of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.
Users noticed difficulties and timeouts last month when adding products to their shopping carts during a promotional sales event. The operations team retrieved the web servers' log files and analyzed the performance data for the Aurora DB cluster. Several web servers were shut down prior to the collection of logs, and the Aurora metrics were insufficient for query performance study.

Which combination of activities must the solutions architect do to increase application performance visibility during times of high traffic? (Select three.)

- A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.
- B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.
- C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis
- D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.
- E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora.
- F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

Commented [LC270]:

Commented [LC271]:

Commented [LC272]:

Question #620

A business serves files to its customers using an SFTP server connected to the Internet. The SFTP server is hosted on a single Amazon EC2 instance that is assigned an Elastic IP address. Customers connect to the SFTP server through the Elastic IP address assigned to it and authenticate using SSH. Additionally, the EC2 instance is connected to a security group that permits access from all client IP addresses.
A solutions architect must create a solution that maximizes availability, minimizes infrastructure management complexity, and causes the least amount of disturbance to consumers that use files. The solution must remain consistent with how consumers interact.

Which solution will satisfy these criteria?

- A. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- B. Disassociate the Elastic IP address from the EC2 instance. Create an Amazon S3 bucket to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted, Internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.
- D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.

Commented [LC273]: A is wrong: you can't attach a EIP to the endpoint of Transfer Family server.

B makes sense.

C, D wrong services involved.

Question #621

The Solutions Architect is responsible for the administration of a serverless application composed of several API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables. Customers report that some application components are sluggish to load dynamic images and that others time out with the '504 Gateway Timeout' issue. The Solutions Architect ensures that the DynamoDB monitoring metrics are within acceptable limits while debugging the problem.

Which of the following approaches is the most efficient way to diagnose these application issues? (Select two.)

- A. Parse HTTP logs in Amazon API Gateway for HTTP errors to determine the root cause of the errors.
- B. Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals.
- C. Parse VPC Flow Logs to determine if there is packet loss between the Lambda function and S3.
- D. Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors.
- E. Parse S3 access logs to determine if objects being accessed are from specific IP addresses to narrow the scope to geographic latency issues.

Commented [LC274]: B and D are correct.
Firstly "A 504 Gateway Timeout" Error means your web server didn't receive a timely response from another server upstream when it attempted to load one of your web pages. Put simply, your web servers aren't communicating with each other fast enough.

This specific issue is addressed in the AWS article "Tracing, Logging and Monitoring an API Gateway API".

https://docs.amazonaws.cn/en_us/apigateway/latest/developerguide/monitoring_overview.html

The article specifically discusses using AWS X-Ray, AWS CloudTrail and AWS CloudWatch as the tools to utilized for debugging in this scenario.

The two options that encompass using AWS CloudWatch and AWS X-Ray are B and D respectively. AWS CloudTrail is not mentioned in any of the answers.

Question #622

A business must design a hybrid DNS solution. This solution will make use of an Amazon Route 53 private hosted zone for the domain cloud.example.com in order to access the resources contained inside VPCs. The company's DNS resolution criteria are as follows:
⇨ On-premises systems should be able to resolve and connect to cloud.example.com.
⇨ All VPCs should be able to resolve cloud.example.com.
Between the on-premises corporate network and AWS Transit Gateway, an AWS Direct Connect link already exists.

Which architecture should the business employ to ensure that these criteria are met with the greatest possible performance?

- A. Associate the private hosted zone to all the VPCs. Create a Route 53 inbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
- B. Associate the private hosted zone to all the VPCs. Deploy an Amazon EC2 conditional forwarder in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the conditional forwarder.
- C. Associate the private hosted zone to the shared services VPC. Create a Route 53 outbound resolver in the shared services VPC. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the outbound resolver.
- D. Associate the private hosted zone to the shared services VPC. Create a Route 53 inbound resolver in the shared services VPC. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.

Commented [LC275]:

Commented [LC276]: Answer is A.

Good explanation on Route53 resolvers here:

https://medium.com/@mda590/an-update-to-hybrid-dns-for-the-enterprise-on-aws-introducing-route-53-resolver-for-hybrid-cloud-74e55d4e67a2

https://4sysops.com/archives/hybrid-dns-between-aws-and-on-prem-with-aws-route-53-resolver/

https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/

Question #623

Your application utilizes an ELB in front of an Auto Scaling set of web/application servers distributed over two AZs, as well as a Multi-AZ RDS Instance for data persistence.
The database CPU is often over 80% used, and 90% of database I/O activities are reads. You recently built a single-node Memcached ElastiCache Cluster to cache frequently accessed database results in order to increase speed. The entire workload is likely to increase by 30% during the following several weeks.

Do you need to make any changes to the architecture in order to ensure high availability or to adapt the application to the expected increased 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.

Commented [LC277]: 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 cachingfocused solution.
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 ... [1]

Question #624

A major organization with hundreds of AWS accounts recently developed a standardized internal procedure for acquiring new Reserved Instances or updating old ones. This approach requires all business units interested in purchasing or modifying Reserved Instances to submit requests for procurement or execution to a dedicated team. Previously, business divisions purchased or modified Reserved Instances in their own AWS accounts independently.

Which combination of activities should be made to proactively enforce the new procedure in the SAFEST manner possible? (Select 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.

Commented [LC278]: A & D is the right answer. First put all accounts into OU and the apply SCP to deny access to the EC2 API that procure new reserved instances or modify existing reserved instances.

Commented [LC279]:

Question #625

A Solutions Architect is in charge of revamping an existing Java program in order to increase its availability, data durability, and scalability. Currently, the application is hosted on a single Amazon EC2 instance with a large amount of RAM. It takes HTTP requests from upstream clients, queues them in memory, and answers with a status code of 200. A second application thread takes items from the queue, processes them, and persists the results to a MySQL instance hosted by Amazon RDS. Each item takes around 90 seconds to complete, the majority of which is spent waiting for external service calls, however the program is designed to handle numerous things concurrently.
The volume of traffic to this service is unpredictably high. During instances of heavy traffic, things may linger in the internal queue for more than an hour while the program works through the backlog.

Additionally, the existing system has concerns with availability and data loss in the event of the failure of a single application node.
Clients that use this service are not modifiable. They anticipate receiving a response to each HTTP request they submit within 10 seconds, at which point the request will time out and be retried.

Which strategy would maximize the system's availability and durability while reducing processing delay and 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 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.

Commented [LC280]:

Question #626

How does Amazon Web Services differentiate itself from other suppliers in the conventional 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.

Commented [LC281]: Let's pretend I never spent 30€ on this batch of questions to see this. It's never going to appear in the exam, hopefully for AWS.

Question #627

Your Fortune 500 firm has conducted a total cost of ownership study, comparing the usage of Amazon S3 against the acquisition of additional gear. As a result, all workers were allowed access to Amazon S3 for personal document storage.

Which of the following will you need to consider in order to implement a solution that combines single sign-on through your corporate AD or LDAP directory and limits access for each user to a defined user folder in a bucket? (Select 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

Commented [LC282]:

Commented [LC283]:

Commented [LC284]:

Question #628

A Solutions Architect is tasked with the responsibility of creating the storage layer for a freshly acquired application. The application will operate on Amazon EC2 instances and will consist of the following layers and specifications:
⇨ A POSIX file system that is shared across several computers serves as the data layer.
⇨ Static file content that needs block storage with more than 100k IOPS at the service layer.

Which AWS service combination will best suit these requirements? (Select 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

Commented [LC285]:

Commented [LC286]: Now also D is feasible, as per ref.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Although, at the time of the question, probably it wasn't possible yet, so I would pick E.

Question #629

A user is using CloudFormation to launch an EC2 instance and then configure it for usage. The user wishes for the ELB and AutoScaling stacks to be created once the EC2 instance has been started and configured appropriately.

How can this be configured by the user?

- 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.

Commented [LC287]: 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.

Reference:
http://aws.amazon.com/cloudformation/faqs

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html

Question #630

The security team must supply an AWS environment to a group of interns in order for them to construct a serverless video transcoding application. Amazon S3, AWS Lambda, Amazon API Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder will be used in this project.
Interns should have the ability to build and configure required resources, but may not have access to establish or alter AWS IAM roles. The Solutions Architect designs a policy and associates it with the group of interns.

How should the security team arrange the environment to enable self-sufficiency for the interns?

- 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.

Commented [LC288]: Answer is A. The best way to make the interns self-sufficient is to create a policy on the intern group that allows them to create or configure the necessary resources like API Gateway, AWS Cognito etc. for their project and assign service roles created by the security team on the services that would be assumed by these services to talk to other services.

Question #631

A solutions architect is tasked with the responsibility of migrating 50 TB of NFS data to Amazon S3. The files are located on a number of NFS file servers around the business network. These are very thick file systems that hold tens of millions of very little files. The system administrators setup the file interface on an AWS Snowball Edge device and are copying data using a shell script.
According to developers, copying data to the Snowball Edge device is very sluggish. The solutions architect feels this is due to the overhead associated with encrypting and transferring all the little data across the network.

What adjustments can be done to increase the speed of data transfer?

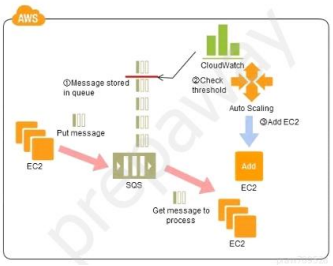
- A. Cluster two Snowball Edge devices together to increase the throughput of the devices.
- B. Change the solution to use the S3 Adapter instead of the file interface on the Snowball Edge device.
- C. Increase the number of parallel copy jobs to increase the throughput of the Snowball Edge device.
- D. Connect directly to the USB interface on the Snowball Edge device and copy the files locally.

Commented [LC289]: It is C for me. Eventhough B sounds very convincing as well. Plus, it provides faster speed then File Interface.

But according to AWS, if transfer is started with File Interface, it should be continued till end. Therefore, opening multiple windows will speed things up. If we want to start over, then obviously S3 Interface would be faster.

Here is the link:
https://docs.aws.amazon.com/snowball/latest/developer-guide/using-fileinterface.html#fileinterface-overview

Question #632



Refer to the architectural diagram above for a batch processing solution that utilizes Simple Queue Service (SQS) to establish a message queue between Amazon Elastic Compute Cloud (EC2) instances that serve as batch processors. Cloud Watch checks the quantity of Job requests (queued messages), and an Auto Scaling group dynamically adds or deletes batch servers depending on Cloud Watch alert criteria.

Which of the following features can you implement cost effectively and efficiently using this architecture?

- 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 worn can continue with recovery of EC2 instances.
- D. Implement fault tolerance against SQS failure by backing up messages to S3.
- E. Implement message passing between EC2 instances within a batch by exchanging messages through SQS.
- F. Coordinate number of EC2 instances with number of job requests automatically thus improving cost effectiveness.
- G. Handle high priority jobs before lower priority jobs by assigning a priority metadata field to SQS messages.

Commented [LC290]: Answer is D
https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KQROiiTiwuq4744rUiV/aws-associate-questions

Question #633

Which of the following is an acceptable Amazon Resource Name (ARN) for IAM?

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

Commented [LC291]: AM ARNs
Most resources have a friendly name (for example, a user named Bob or a group named Developers). However, the permissions policy language requires you to specify the resource or resources using the following Amazon Resource Name (ARN) format.

arn:partition:service:region:account:resource
Where:

partition identifies the partition that the resource is in. For standard AWS Regions, the partition is aws. If you have resources in other partitions, the partition is aws-partitionname. For example, the partition for resources in the China (Beijing) Region is aws-cn. You cannot delegate access between accounts in different partitions.

service identifies the AWS product. For IAM resources, this is always iam.

region is the Region the resource resides in. For IAM resources, this is always kept blank.

account is the AWS account ID with no hyphens (for example, 123456789012).

resource is the portion that identifies the specific resource by name.

Question #634

Your business stores millions of confidential transactions in thousands of 100-GB files that must be protected in transit and at rest. Analysts rely on subsets of files, which may use up to 5 TB of storage, in order to develop simulations that can be used to guide business choices.
You must develop an AWS solution that can support both long-term storage and in-flight subsets of data cost efficiently.

Which strategy is most likely to accomplish these goals?

- 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.

Commented [LC292]:

Question #635

When you resize an Amazon RDS database instance, Amazon RDS upgrades it during the following maintenance window. If you want to apply the upgrade immediately rather than during the maintenance time, indicate the option.

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

Commented [LC293]: D
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html

Using the Apply Immediately Parameter
When you modify a DB instance, you can apply the changes immediately. To apply changes immediately, you select the Apply Immediately option in the AWS Management Console, you use the --apply-immediately parameter when calling the AWS CLI, or you set the ApplyImmediately parameter to true when using the Amazon RDS API.

Question #636

A business maintains a major Amazon S3 bucket, which gets thousands of items daily. The organization must duplicate these assets into several additional S3 buckets using multiple AWS accounts. A solutions architect is developing a new AWS Lambda function that is called when an item is produced in the main bucket and duplicates it to the target buckets. It is not necessary to reproduce the items in real time. Concerns have been expressed that this function may have an adverse effect on other key Lambda functions owing to Lambda's regional concurrency restriction.

How can the solutions architect assure that the addition of this new Lambda function has no adverse effect on other key Lambda functions?

- A. Set the new Lambda function reserved concurrency limit to ensure the executions do not impact other critical Lambda functions. Monitor existing critical Lambda functions with Amazon CloudWatch alarms for the Throttles Lambda metric.
- B. Increase the execution timeout of the new Lambda function to 5 minutes. Monitor existing critical Lambda functions with Amazon CloudWatch alarms for the Throttles Lambda metric.
- C. Configure S3 event notifications to add events to an Amazon SQS queue in a separate account. Create the new Lambda function in the same account as the SQS queue and trigger the function when a message arrives in the queue.
- D. Ensure the new Lambda function implements an exponential backoff algorithm. Monitor existing critical Lambda functions with Amazon CloudWatch alarms for the Throttles Lambda metric.

Commented [LC294]: A -
https://docs.aws.amazon.com/lambda/latest/dg/configuration-concurrency.html

When a function has reserved concurrency, no other function can use that concurrency. >>>Reserved concurrency also limits the maximum concurrency for the function<<<, and applies to the function as a whole, including versions and aliases.

To be honest bothering a new account (answer C) without setting the permissions, as it may seem right (but still permissions are required), it's a little bit weird.

Question #637

You just joined a small business that is developing sensors to monitor street noise and urban air quality. For three months, the business has been piloting a deployment of about 100 sensors, with each sensor uploading 1KB of sensor data per minute to an AWS backend.
You recorded a maximum of 10 IOPS on the database during the pilot and saved an average of 3GB of sensor data each month in the database.
The current deployment includes a load-balanced, auto-scaling Ingestion layer built on Amazon EC2 instances and a PostgreSQL RDS database with 500GB of standard storage.
The pilot is deemed a success, and your CEO has garnered the interest of several prospective investors. The business strategy calls for the deployment of at least 100K sensors, which the backend must handle. Additionally, you must keep sensor data for a minimum of two years in order to compare year over year improvements.
To receive finance, you must ensure that your platform fits these criteria and allows for future growth.

Which configuration will satisfy 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

Commented [LC295]: My answer is B. Even though Redshift is capable of storing data. It is certainly not capable of handling currency for 100K sensor data (At least 1000 TPS) or it is built for small frequent transactions. However, DynamoDB can easily handle 1000 WPS. Then, moving the data from DynamoDB to Redshift for long term analytics is the right approach

Question #638

Currently, you are running a web application. In the Amazon Web Services (AWS) US-East region. The application is implemented using an auto-scaled layer of Amazon EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has charged you with developing a logging system that is both dependable and durable for tracking changes to your EC2, IAM and RDS resources. Your log data's integrity and confidentiality must be ensured by the solution.

Which of these alternatives would you suggest?

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

Commented [LC296]: A.
1 a new CT trail + 1 new S3 bucket + global services option selected + IAM roles + bucket policies + MFA Delete.

Global services option is not needed to select when creates using AWS console, but it will need to set --is-multi-region-trail true to enable global services if you create from aws cli.

Question #639

Your firm is headquartered in Tokyo and has branch offices located across the globe. It uses a logistics software that is multi-regionally deployed on AWS in Japan, Europe, and the United States. The logistic software is built on a three-tier design and presently stores data in MySQL 5.6. Each area has its own database in place.
In the headquarters region, you run an hourly batch process that reads data from all regions and generates cross-regional reports that are sent to all offices. This batch process must be finished as rapidly as possible to maximize logistics.

How do you structure the database architecture to ensure that it satisfies 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

Commented [LC297]: A.
Read Replicas for "as fast as possible" requirement.

Question #640

Which of the following cannot be used to manage and administer Amazon ElastiCache?

- A. AWS software development kits (SDKs)
- B. Amazon S3
- C. ElastiCache command line interface (CLI)
- D. AWS CloudWatch

Commented [LC298]: Perhaps an outdated question. My guess is on B.

Question #641

User photographs are uploaded to Amazon S3 for processing by a media storage application. According to end users, some submitted photographs are not being processed correctly. The Application Developers examine the logs and discover that AWS Lambda is having execution troubles when thousands of users are concurrently connected to the system. Issues arise as a result of:

⇨ Limits around concurrent executions.
⇨ The performance of Amazon DynamoDB when saving data.

Which steps may be performed to improve the application's performance and reliability? (Select 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.

Commented [LC299]: BD
A\C: Read is not the problem here. (when saving data...)
B: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.requests
D: https://aws.amazon.com/blogs/compute/robust-serverless-application-design-with-aws-lambda-dlq/c
E: Does not solve the problem. Issue does not lie in the ingestion, it lies with processing.

Commented [LC300]:

Question #642

An e-commerce business is modernizing its IT infrastructure and intends to use AWS services. The company's chief information officer (CIO) has tasked a Solutions Architect with designing a simple, highly available, and loosely linked order processing application. Orders are received and processed by the application before being stored in an Amazon DynamoDB database. The application receives intermittent traffic and should be able to grow during marketing campaigns in order to process orders quickly.

Which of the following approaches is the MOST RESPONSIBLE method for meeting the requirements?

- A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
- B. Receive the orders in an Amazon SQS queue and trigger an AWS Lambda function to process them.
- C. Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container to process them.
- D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

Commented [LC301]: Looks like B, C and D are correct. But I prefer B since SQS provides reliability & Lambda gives scalability.
C (an ECS container) & D (EC2 instances) don't give HA & scale.

Question #643

A business is developing an electronic document management system that will allow users to upload documents. The application stack is completely serverless and is hosted on Amazon Web Services in the eu-central-1 Region. The system consists of a web application that is delivered through an Amazon CloudFront distribution with an Amazon S3 origin.

The web application interfaces with regional endpoints of the Amazon API Gateway. The API Gateway APIs invoke AWS Lambda services, which store metadata in an Amazon Aurora Serverless database and document content in an S3 bucket.

The business is thriving and just completed a proof of concept with its major client. Outside of Europe, the corporation must improve latency.

Which combination of acts satisfies these criteria? (Select two.)

- A. Enable S3 Transfer Acceleration on the S3 bucket. Ensure that the web application uses the Transfer Acceleration signed URLs.
- B. Create an accelerator in AWS Global Accelerator. Attach the accelerator to the CloudFront distribution.
- C. Change the API Gateway Regional endpoints to edge-optimized endpoints.
- D. Provision the entire stack in two other locations that are spread across the world. Use global databases on the Aurora Serverless cluster.
- E. Add an Amazon RDS proxy between the Lambda functions and the Aurora Serverless database.

Commented [LC302]: BC - An edge-optimized API endpoint is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP). This is the default endpoint type for API Gateway REST APIs.

Commented [LC303]:

Question #644

A media business uses AWS to host a high-traffic news website. The front end of the website is entirely composed of HTML and JavaScript. All dynamic material is loaded dynamically using asynchronous JavaScript queries to a specialized backend architecture.

The front end is hosted on four Amazon EC2 instances. The dynamic backend is containerized and operates on an Amazon Elastic Container Service (Amazon ECS) cluster comprised of Auto Scaling EC2 instances. The ECS tasks are performed behind a load balancer (ALB).

Which solutions should a solutions architect suggest for cost optimization? (Select two.)

- A. Migrate the front end of the website to an Amazon S3 bucket. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the distribution's origin.
- B. Deploy an Amazon CloudFront distribution. Configure the distribution to use the ALB endpoint as the origin.
- C. Migrate the front-end services to the ECS cluster. Increase the minimum number of nodes in the Auto Scaling group.
- D. Turn on Auto Scaling for the front-end EC2 instances. Configure a new listener rule on the ALB to serve the front end.
- E. Migrate the backend of the website to an Amazon S3 bucket. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the distribution's origin.

Commented [LC304]:

Commented [LC305]:

Question #645

A business purchases licensed software. A software license may be assigned to just one MAC Address. The organization will host the software on AWS.

How can the organization meet the licensing requirement when the MAC address of each instance is changed when it is started, halted, or 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.

Commented [LC306]: 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.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

Question #646

A business has deployed an application to a variety of AWS environments, including production and testing. The organization maintains distinct accounts for production and testing, and users may establish extra application users as required for team members or services. The Security team has requested increased isolation between production and testing environments, centralized control over security credentials, and improved management of permissions across environments from the Operations team.

Which of the following methods would fulfill this objective the MOST SECURELY?

- 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.

Commented [LC307]: A

A: By centralizing users to a single account, a user can access the prod and test using assume role. This ensures that all actions are properly logged and is the most secure. Adapted from this article:

https://aws.amazon.com/blogs/security/how-to-centralize-and-automate-iam-policy-creation-in-sandbox-development-and-test-environments/

B: This means the test users will still need to be created. The problem with test users is always security. Who is the actual person behind the scene carrying out that specific actions? This is unlikely the most secure option.

C: Any answers that is asking you to write a script is very unlikely to be the answer.

D: This seems to be able to work too which is similar to A. But the Security team already asked for "better isolation with centralized controls". Hence, I chose A.

Question #647 (EXAM)

A business with many Amazon Web Services accounts makes use of AWS Organizations and service control rules (SCPs). The following SCP was generated by an administrator and associated to an organizational unit (OU) that holds the AWS account 1111-1111-1111:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenyCloudTrail",
            "Effect": "Deny",
            "Action": "cloudtrail:*",
            "Resource": "*"
        }
    ]
}
```

Developers in account 1111-1111-1111 report being unable to build Amazon S3 buckets.

How should the Administrator proceed in resolving this issue?

- 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.

Commented [LC308]: C

A. It will give other people access of creating S3 bucket.
B. It doesn't comply with organization's rule by removing accournt from OU. And it won't work either.
C. Add required access to Developers only, not affecting others, right option.
D. Provide people to change cloudtrail, which should be prohibited.

Question #648

In the context of the IAM service, a GROUP is defined as:

- 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.

Commented [LC309]: 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 #649

After your Lambda function has been running for some time, you'll want to examine certain metrics to see how well it's functioning. You'll want to accomplish this using the AWS CLI.

Which of the following commands must be performed to get access to these metrics using the AWS Command Line Interface (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

Commented [LC310]: https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/list-metrics.html
https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/get-metric-statistics.html

Question #650

A corporation has an on-premises data center with a High-Performance Computing (HPC) cluster that executes thousands of tasks in parallel for one week each month, processing petabytes of photos. The photos are archived on a network file server and duplicated to a disaster recovery location. The on-premises data center has reached capacity and has begun spreading the tasks over the month in order to maximize the use of the cluster, resulting in a delay in work completion.

The firm has tasked its Solutions Architect with developing a cost-effective solution on AWS that would enable it to go beyond its present capacity of 5,000 cores and 10 petabytes of data. The solution must be as low-maintenance as possible while maintaining the existing degree of durability.

Which option will best fulfill the needs of the business?

- A. Create a container in the Amazon Elastic Container Registry with the executable file for the job. Use Amazon ECS with Spot Fleet in Auto Scaling groups. Store the raw data in Amazon EBS SC1 volumes and write the output to Amazon S3.
- B. Create an Amazon EMR cluster with a combination of On Demand and Reserved Instance Task Nodes that will use Spark to pull data from Amazon S3. Use Amazon DynamoDB to maintain a list of jobs that need to be processed by the Amazon EMR cluster.
- C. Store the raw data in Amazon S3, and use AWS Batch with Managed Compute Environments to create Spot Fleets. Submit jobs to AWS Batch Job Queues to pull down objects from Amazon S3 onto Amazon EBS volumes for temporary storage to be processed, and then write the results back to Amazon S3.
- D. Submit the list of jobs to be processed to an Amazon SQS to queue the jobs that need to be processed. Create a diversified cluster of Amazon EC2 worker instances using Spot Fleet that will automatically scale based on the queue depth. Use Amazon EFS to store all the data sharing it across all instances in the cluster.

Commented [LC311]: C

https://aws.amazon.com/blogs/industries/building-a-scalable-image-processing-pipeline-for-image-based-transcriptomics/

https://docs.aws.amazon.com/wellarchitected/latest/high-performance-computing-lens/batch-based-architecture.html

Question #651

What is the default maximum number of BGP advertised routes per route table in Amazon VPC?

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

Commented [LC312]: The maximum number of BGP advertised routes allowed per route table is 100.
Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html

Question #652

A business wishes to operate Amazon EC2 instances only from AMIs that have been pre-approved by the information security department. The development team uses an agile continuous integration and deployment approach that is invulnerable to the solution's stuttering.

Which strategy imposes the necessary restrictions with the LEAST amount of influence on the development process? (Select 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.

Commented [LC313]: AD
https://aws.amazon.com/blogs/devops/aws-config-checking-for-compliance-with-new-managed-rule-options/

"AWS Config rules can now check that running instances are using approved Amazon Machine Images, or AMIs. You can specify a list of approved AMI by ID or provide a tag to specify the list of AMI Ids."

Commented [LC314]:

Question #653

A financial institution is doing market simulations on a high-performance computing cluster powered by Amazon EC2 instances. When instances are started, a DNS record must be established in an Amazon Route 53 private hosted zone. After instances are terminated, the DNS record must be deleted.
Currently, the organization creates the DNS record using a mix of Amazon CloudWatch Events and AWS Lambda. While the approach worked fine in testing with small clusters, in production with clusters comprising thousands of instances, the organization encounters the following Lambda log error:
HTTP 400 status code (Bad request).
Additionally, the response header contains a status code element with the value "Throttling" and a status message element with the value "Rate exceeded."

Which measures should the Solutions Architect do in combination to overcome these issues? (Select three.)

- A. Configure an Amazon SQS FIFO queue and configure a CloudWatch Events rule to use this queue as a target. Remove the Lambda target from the CloudWatch Events rule.
- B. Configure an Amazon Kinesis data stream and configure a CloudWatch Events rule to use this queue as a target. Remove the Lambda target from the CloudWatch Events rule.
- C. Update the CloudWatch Events rule to trigger on Amazon EC2 Instance Launch Successful and Instance Terminate Successful events for the Auto Scaling group used by the cluster.
- D. Configure a Lambda function to retrieve messages from an Amazon SQS queue. Modify the Lambda function to retrieve a maximum of 10 messages then batch the messages by Amazon Route 53 API call type and submit. Delete the messages from the SQS queue after successful API calls.
- E. Configure an Amazon SQS standard queue and configure the existing CloudWatch Events rule to use this queue as a target. Remove the Lambda target from the CloudWatch Events rule.
- F. Configure a Lambda function to read data from the Amazon Kinesis data stream and configure the batch window to 5 minutes. Modify the function to make a single API call to Amazon Route 53 with all records read from the kinesis data stream.

Commented [LC315]: CDE is perfect answer.

The errors in the Lambda logs indicate that throttling is occurring. Throttling is intended to protect your resources and downstream applications. Though Lambda automatically scales to accommodate incoming traffic, functions can still be throttled for various reasons.

In this case it is most likely that the throttling is not occurring in Lambda itself but in API calls made to Amazon Route 53. In Route 53 you are limited (by default) to five requests per second per AWS account. If you submit more than five requests per second, Amazon Route 53 returns an HTTP 400 error (Bad request). The response header also includes a Code element with a value of Throttling and a Message element with a value of Rate exceeded.

The resolution here is to place the data for the DNS records into an SQS queue where they can buffer. AWS Lambda can then poll the queue and process the messages, making sure to batch the messages to reduce the likelihood of receiving more errors.

Question #654

What sorts of identities are supported by Amazon Cognito identity pools?

- 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.

Commented [LC316]:

Commented [LC317]:

Commented [LC318]: 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 #655

A cloud-based application will be transferred from on-premises. The application is composed of a single Elasticsearch virtual machine with data source feeds from non-migrated local systems and a Java web application running on Apache Tomcat on three virtual machines. Elasticsearch now consumes 1 TB of storage space out of a total of 16 TB available, and the web application is updated every four months. The web application is accessible through the Internet by several users. A 10Gbit AWS Direct Connect connection has been built, and the application may now be transferred within a 48-hour planned change window.

Which option will have the MINIMUM effect on Operations personnel 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.

Commented [LC319]: A- Will require management of EC2 nodes for ES post migration
B - ES can't be source for DMS as it can be only a target
C - EC2 VMs will be required to manage post migration
D - Correct Answer

Question #656 (SKIP)

What is the maximum number of Cache Nodes that you may operate in Amazon ElastiCache by default?

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

Commented [LC320]: https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/quota-limits.html

Nodes per Region → 300
Nodes per cluster per instance type (Redis cluster mode enabled) → 90
Nodes per shard (Redis cluster mode disabled) → 6

Question #657 (SKIP)

How many g2.2xlarge on-demand instances can a customer operate in a single region without obtaining AWS clearance for a limit increase?

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

Commented [LC321]: Outdated question

https://awslimitchecker.readthedocs.io/en/latest/limits.html#ec2-standard-regions

Question #658

You've created an Amazon EC2 instance and connected four (4) 500 GB EBS Provisioned IOPS volumes. The EC2 instance is optimized for EBS and offers a throughput of 500 Mbps between EC2 and EBS. The four EBS volumes are set in RAID 0, and each Provided IOPS volume is provisioned with 4,000 IOPS (4,000 16KB reads or writes), giving the instance a total of 16,000 random IOPS. The EC2 instance initially performs at the desired rate of 16,000 IOPS random read and write. Later on, to boost the instance's overall random I/O performance, you add two 500 GB EBS Provisioned IOPS volumes to the RAID. Each volume, like the original four, is provisioned to 4,000 IOPS, for a total of 24,000 IOPS on the EC2 instance. Monitoring indicates that the CPU usage of the EC2 instance went from 50% to 70%, while the total random IOPS observed at the instance level remained constant.

What is the issue and what is a viable solution?

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

Commented [LC322]: A.

According to
https://aws.amazon.com/ebs/volume-types/
500GB gp2 can only provide 1500 IOPS, so it has to be io1 or io2, then ebs isn't the bottleneck.
So, the bottleneck is the instance.

Instances types:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-optimized.html

Question #659

Which EC2 feature enables the user to cluster Cluster Compute instances?

- A. Cluster group
- B. Cluster security group
- C. GPU units
- D. Cluster placement group

Commented [LC323]: The Amazon EC2 cluster placement group functionality allows users to group cluster compute instances in clusters.
Reference:
https://aws.amazon.com/ec2/faqs/

Question #660

A firm has a social networking application for picture sharing. To provide a uniform user experience, the business does some image processing on user-uploaded photographs prior to publishing them on the program. The image processing is accomplished via the use of a collection of Python libraries.
As of now, the architecture is as follows:
⇨ The image processing Python code runs in a single Amazon EC2 instance and stores the processed images in an Amazon S3 bucket named ImageBucket.
⇨ The front-end application, hosted in another bucket, loads the images from ImageBucket to display to users.
With worldwide development aspirations, the firm want to modify its present architecture in order to expand the application for higher demand while also reducing administration complexity as the program grows.

Which adjustments should a solutions architect make in combination? (Select two.)

- A. Place the image processing EC2 instance into an Auto Scaling group.
- B. Use AWS Lambda to run the image processing tasks.
- C. Use Amazon Rekognition for image processing.
- D. Use Amazon CloudFront in front of ImageBucket.
- E. Deploy the applications in an Amazon ECS cluster and apply Service Auto Scaling.

Commented [LC324]: Going with B and D even though B may timeout before the image processing has been completed.

Commented [LC325]:

Question #661

AWS Organizations is used by a business to manage one parent account and nine member accounts. The number of member accounts is likely to expand in lockstep with the growth of the firm. For compliance considerations, a security engineer has requested consolidation of AWS CloudTrail logs into the parent account. Existing logs in Amazon S3 buckets inside each member account should not be lost. All subsequent member accounts should adhere to the logging approach.

What operationally efficient solution satisfies these criteria?

- A. Create an AWS Lambda function in each member account with a cross-account role. Trigger the Lambda functions when new CloudTrail logs are created and copy the CloudTrail logs to a centralized S3 bucket. Set up an Amazon CloudWatch alarm to alert if CloudTrail is not configured properly.
- B. Configure CloudTrail in each member account to deliver log events to a central S3 bucket. Ensure the central S3 bucket policy allows PutObject access from the member accounts. Migrate existing logs to the central S3 bucket. Set up an Amazon CloudWatch alarm to alert if CloudTrail is not configured properly.
- C. Configure an organization-level CloudTrail in the parent account to deliver log events to a central S3 bucket. Migrate the existing CloudTrail logs from each member account to the central S3 bucket. Delete the existing CloudTrail and logs in the member accounts.
- D. Configure an organization-level CloudTrail in the parent account to deliver log events to a central S3 bucket. Configure CloudTrail in each member account to deliver log events to the central S3 bucket.

Commented [LC326]: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html

Question #662

Users may bid on collectable objects on an auction website. According to the auction regulations, each bid must be processed only once and in the sequence in which it was received. The present approach is based on an Amazon EC2 web server fleet that writes bid records to Amazon Kinesis Data Streams. A single t2.large instance is configured with a cron job that runs the bid processor, which receives and analyzes incoming bids from Kinesis Data Streams. Although the auction site is gaining popularity, users are reporting that certain bids are not being registered. Troubleshooting suggests that the bid processor is inefficient during high demand hours, crashes periodically during processing, and occasionally loses track of which records are being processed.

What adjustments should be made to increase the reliability of bid processing?

- 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.

Commented [LC327]: https://aws.amazon.com/kinesis/data-streams/faqs/

Order apparently is maintained as per ref.

(Search for the word Order)

Question #663

You may restrict access to S3 buckets and objects using the following:

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

Commented [LC328]: All the above - IAM at user/group level, Bucket Polices at Bucket level, ACLs at Object level

Question #664

You've been entrusted with the responsibility of migrating a legacy application from a virtual machine hosted in your datacenter to an Amazon VPC. Regrettably, this app needs access to many on-premises services, and the person who set it no longer works for your firm. Worse still, there is no documentation.

What enables the application operating inside the VPC to communicate with and access its internal dependencies without requiring reconfiguration? (Select three.)

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

Commented [LC329]: A, D, F.
First you would like to move your on-premise server to AWS server (for ex, EC2), it require VM import to import our image to AWS EC2. So, F is mandatory.

This server requires connecting back to your data center network (services), so it requires connection, in this case Direct Connect, so A.

The connection is internal from AWS VPC to your data center through DX, so Route53 or EIP (which are for external/Internet) is not essential here.

When internally connected, you need IP of your AWS machine not conflict with data center services IPs, so it's D

Commented [LC330]:

Commented [LC331]:

Question #665

A business is now adopting AWS Organizations to limit its developers access Amazon EC2, Amazon S3, and Amazon DynamoDB. Developers is a distinct organizational entity (OU). On the Developers account, the Solutions Architect has implemented the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "AllowDynamoDB",
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "*"
        },
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

After deploying this policy, IAM users in the Developers account may continue to utilize AWS services that are not included in the policy.

What should the Solutions Architect do to prevent Developers from accessing services that are not covered by this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained.
- B. Remove the FullAWSAccess SCP from the Developer account's OU.
- C. Modify the FullAWSAccess SCP to explicitly deny all services.
- D. Add an explicit deny statement using a wildcard to the end of the SCP.

Commented [LC332]: This does the job.

Question #666

A business formerly relied on a third-party supplier for its content delivery network but just switched to Amazon CloudFront. The development team is committed to provide the best possible performance for the worldwide user base. The organization makes use of a content management system (CMS) to handle both static and dynamic information.
The CMS is hidden behind an Application Load Balancer (ALB), which is configured as the distribution's default origin. Static materials are supplied from a bucket on Amazon S3.
Although the Origin Access Identity (OAI) was successfully constructed and the S3 bucket policy was adjusted to permit the GetObject operation from the OAI, static assets are generating a 404 error.

Which measures should the solutions architect do in combination to correct the error? (Select two.)

- A. Add another origin to the CloudFront distribution for the static assets.
- B. Add a path-based rule to the ALB to forward requests for the static assets.
- C. Add an RTMP distribution to allow caching of both static and dynamic content.
- D. Add a behavior to the CloudFront distribution for the path pattern and the origin of the static assets.
- E. Add a host header condition to the ALB listener and forward the header from CloudFront to add traffic to the allow list.

Commented [LC333]:

Commented [LC334]:

Question #667

A solutions architect is developing a publicly available online application that will be distributed through Amazon CloudFront and will originate from an Amazon S3 website endpoint. After deploying the solution, the website displays an Error 403: Access Denied notice.

How should the solutions architect proceed to resolve the issue? (Select two.)

- A. Remove the S3 block public access option from the S3 bucket.
- B. Remove the requester pays option from the S3 bucket.
- C. Remove the origin access identity (OAI) from the CloudFront distribution.
- D. Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA).
- E. Disable S3 object versioning.

Commented [LC335]: A and C
If you don't want to allow public (anonymous) access to your S3 objects, then change your configuration to use the S3 REST API endpoint as the origin of your distribution. Then, configure your distribution and S3 bucket to restrict access using an origin access identity (OAI).
https://aws.amazon.com/premiumsupport/knowledge-center/s3-website-cloudfront-error-403/

Commented [LC336]:

Question #668

A Solutions Architect is creating a network solution for a corporation whose applications are hosted in a Northern Virginia data center. The company's data center applications demand predictable performance in comparison to those operating in a virtual private cloud (VPC) in us-east-1 and a secondary VPC in us-west-2 inside the same account. The company's data center is colocated in a US-east-1 AWS Direct Connect facility. The organization has already placed an order for an AWS Direct Connect connection and created a cross-connect.

Which option satisfies the criteria AT THE CHEAPEST PRICE?

- 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.

Commented [LC337]: Answer is definitely A. Let the US-WEST2 take advantage of the existing DX connection via a direct connect gateway via respective AZ's Virtual Private Gateway (VIF/s).

B makes no sense.

C doesn't answer lowest cost

D is the most expensive option

Doc direct connect:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html

Question #669

The processing team of a business has an AWS account with a production application. The application is hosted on Amazon EC2 instances that are routed via a Network Load Balancer (NLB). Private subnets inside a VPC in the eu-west-1 Region are used to host the EC2 instances. A CIDR block of 10.0.0.0/16 was allocated to the VPC. Recently, the billing team built a new AWS account and deployed an application on EC2 instances housed on private subnets under a VPC in the eu-central-1 Region. The new virtual private cloud is allocated the CIDR block 10.0.0.0/16.

Secure communication between the processing application and the billing application over a proprietary TCP port is required.

What should a solutions architect do to ensure that this need is met with the MINIMUM amount of operational work possible?

- A. In the billing team's account, create a new VPC and subnets in eu-central-1 that use the CIDR block of 192.168.0.0/16. Redeploy the application to the new subnets. Configure a VPC peering connection between the two VPCs.
- B. In the processing team's account, add an additional CIDR block of 192.168.0.0/16 to the VPC in eu-west-1. Restart each of the EC2 instances so that they obtain a new IP address. Configure an inter-Region VPC peering connection between the two VPCs.
- C. In the billing team's account, create a new VPC and subnets in eu-west-1 that use the CIDR block of 192.168.0.0/16. Create a VPC endpoint service (AWS PrivateLink) in the processing team's account and an interface VPC endpoint in the new VPC. Configure an inter-Region VPC peering connection in the billing team's account between the two VPCs.
- D. In each account, create a new VPC with the CIDR blocks of 192.168.0.0/16 and 172.16.0.0/16. Create inter-Region VPC peering connections between the billing team's VPCs and the processing team's VPCs. Create gateway VPC endpoints to allow traffic to route between the VPCs.

Commented [LC338]: So, it should work like this. Prod's account has a Private Link (because it's where the application resides) which connects to the vpt endpoint of the new VPC (192.168.x.x). Then, this VPC (192.168.x.x) is connected to the other VPC of the same account (billing account) via VPC Peering (10.0.0.0/16)

Question #670

Within a firm, a development team is releasing new APIs as serverless apps. At the moment, the team is utilizing the AWS Management Console to deploy resources for Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. A Solutions Architect has been charged with automating future serverless API installations.

How is this possible?

- 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.

Commented [LC339]: https://aws-quickstart.s3.amazonaws.com/quickstart-trek10-serverless-enterprise-cicd/doc/serverless-cicd-for-the-enterprise-on-the-aws-cloud.pdf

Question #671

Which of the following attributes of Amazon VPC subnets are true? (Select 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.

Commented [LC340]: Of course it's BD
E is wrong, without igw, a subnet can't communicate with internet.
And a private subnet has no igw

Commented [LC341]:

Question #672

You are creating a URL whitelisting system for a business that want to limit outbound HTTPS connections from its EC2-hosted apps to particular sites. You setup a single EC2 instance running proxy software to accept traffic from all subnets and EC2 instances inside the VPC. You configure the proxy to forward traffic only to the domains specified in its whitelist setting. You have a nightly or ten-minute maintenance window during which all instances download new software upgrades. Each update is around 200MB in size, and there are 500 instances in the VPC that fetch updates on a regular basis. After a few days, you may discover that certain computers are unable to download some, but not all, of their scheduled updates during the maintenance window. The download URLs for these updates are appropriately displayed in the proxy's whitelist setup, and they can be accessed manually on the instances through a web browser.

What may be going on? (Select two.)

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

Question #673

Which of the following is an AWS Storage service? (Select two.)

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

Question #674

A firm intends to implement a new business analytics application that will need 10,000 hours of compute time each month. Flexible availability of computational resources is acceptable, but they must be as cost-effective as feasible. Additionally, the organization will offer a reporting service for distributing analytics results, which must be available at all times.

How should the Solutions Architect approach developing a solution that satisfies these requirements?

- A. Deploy the reporting service on a Spot Fleet. Deploy the analytics application as a container in Amazon ECS with AWS Fargate as the compute option. Set the analytics application to use a custom metric with Service Auto Scaling.
- B. Deploy the reporting service on an On-Demand Instance. Deploy the analytics application as a container in AWS Batch with AWS Fargate as the compute option. Set the analytics application to use a custom metric with Service Auto Scaling.
- C. Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option. Deploy the analytics application on a Spot Fleet. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the Spot Fleet.
- D. Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option. Deploy the analytics application on an On-Demand Instance and purchase a Reserved Instance with a 3-year term. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the On-Demand Instance.

Commented [LC342]: That is a nicely worded question.

so we are limiting outbound traffic. There is a proxy doing destination filtering.

Some updates fail. Indicating that some are successful and therefore the basic design & networking is correct.

a 10-minute window to pass 200MB x 500 instances = 100GB of traffic. I would call that as a lot, especially for a generic server based service.

So probably a bottleneck of some sort

E./ We don't know the instance type, The NIC would not normally be the 1st place I look for a bottle neck, and I am not convinced that you can do LACP (Link Aggregation of ether-channel) in instances since you need to configure the switch connections which we don't have access to. (in my opinion a Low Probability answer)

D./ I don't know enough about this sort of proxy configuration. However, it is unlikely to be a store and forward configuration, more likely just header examination of the 1st packet and then fast forwarding of the bulk of the stream. So while some buffer space will be needed I am not convinced about this answer (in my opinion a Low Probability answer)

C./ Since only some machines fail and manual checks are successful I would discount this on my 1st pass of the answers

B./ We don't have any information about id the hosts are in a public or private subnet. If they are in a private subnet, then a NAT would be needed. This answer is plausible (this would be a prefered answer for me)

A./ We don't have any information about id the hosts are in a public or private subnet. Either way the Proxy itself could be bottle neck on any of the core resources. This answer is plausible (this would be a prefered answer for me)

Commented [LC343]:

Commented [LC344]: https://aws.amazon.com/products/storage/

Commented [LC345]:

Commented [LC346]: C. Use spot instances for analytics workload. Reporting services need to be up all the time, hence should run on a reliable instance type that will not terminate on its own.

A Spot Fleet is set of Spot Instances and optionally On-Demand Instances that is launched based on criteria that you specify. The Spot Fleet selects the Spot capacity pools that meet your needs and launches Spot Instances to meet the target capacity for the fleet. By default, Spot Fleets are set to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated. You can submit a Spot Fleet as a one-time request, which does not persist after the instances have been terminated. You can include On-Demand Instance requests in a Spot Fleet request.

Question #675

During a security assessment of a Service team's application, a Solutions Architect finds that the AWS Lambda function code contains a username and password for an Amazon RDS database and a set of AWS IAM user credentials. The Lambda function connects to the database using the login and password, and it connects to AWS services using the IAM credentials under a separate management account.

The Solutions Architect is afraid that the credentials might be misused by anybody who can examine the Lambda code. The management account and the account for the service team are located in distinct AWS Organizations organizational units (OUs).

Which combination of modifications should the Solutions Architect make to increase the security of the solution? (Select two.)

- A. Configure Lambda to assume a role in the management account with appropriate access to AWS.
- B. Configure Lambda to use the stored database credentials in AWS Secrets Manager and enable automatic rotation.
- C. Create a Lambda function to rotate the credentials every hour by deploying a new Lambda version with the updated credentials.
- D. Use an SCP on the management account's OU to prevent IAM users from accessing resources in the Service team's account.
- E. Enable AWS Shield Advanced on the management account to shield sensitive resources from unauthorized IAM access.

Commented [LC347]: A/B
Assuming the role is the right way to do it. And SSM is good for storing DB credentials
https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/

D is wrong as users from one account cannot access resources from another account if not allowed through cross-account access using assumed roles. There's no need to use SCP for deny
E is wrong as shield is used for ddos protection
C does not make sense with hourly redeploying of lambda

Commented [LC348]:

Question #676

On AWS, a user hosts a public website. The user wishes to host both the database and the application server inside an AWS VPC. The user wishes to configure a database that is capable of connecting to the Internet in order to perform patch upgrades but is unable to accept any requests from the internet.

How does the user configure this?

- 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.

Commented [LC349]: D without any doubts.

Question #677

A corporation has launched a new version of its website with an Asian and South American audience in mind. The website's media assets are stored on Amazon S3 and distributed through Amazon CloudFront to enhance end-user performance. However, customers are having a difficult time logging in since the authentication service is only accessible in the AWS Region us-east-1.

How can the Solutions Architect enhance the login experience while maintaining a high level of security and performance with little administration effort?

- 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.

Commented [LC350]: C
There are several benefits to using Lambda@Edge for authorization operations. First, performance is improved by running the authorization function using Lambda@Edge closest to the viewer, reducing latency and response time to the viewer request. The load on your origin servers is also reduced by offloading CPU-intensive operations such as verification of JSON Web Token (JWT) signatures. Finally, there are security benefits such as filtering out unauthorized requests before they reach your origin infrastructure.

https://aws.amazon.com/blogs/networking-and-content-delivery/authorizationedge-how-to-use-lambdaedge-and-json-web-tokens-to-enhance-web-application-security/

Question #678 (EXAM)

A business is creating a gene reporting device that will gather genetic data to aid researchers in the collection of huge samples of data from a varied population. The gadget will transmit 8 KB of genomic data per second to a data platform, which will be responsible for processing and analyzing the data and communicating the results to researchers. The data platform must comply with the following specifications:
⇨ Analyze incoming genomic data in near-real time
⇨ Ascertain that the data is adaptable, parallel, and durable
⇨ Deliver processed data to a data warehouse

Which approach should a solutions architect use in order to satisfy these requirements?

- A. Use Amazon Kinesis Data Firehouse to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance.
- B. Use Amazon Kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift cluster using Amazon EMR.
- C. Use Amazon S3 to collect the inbound device data, analyze the data from Amazon SQS with Kinesis, and save the results to an Amazon Redshift cluster.
- D. Use an Amazon API Gateway to put requests into an Amazon SQS queue, analyze the data with an AWS Lambda function, and save the results to an Amazon Redshift cluster using Amazon EMR.

Commented [LC351]: B. Redshift is the data-warehouse. EMR to do the data transformation. Kinesis for real-time data transfer.

Question #679

A business uses AWS to host a three-tier application that includes a web server, an application server, and an Amazon RDS MySQL database instance. A solutions architect is developing a disaster recovery (DR) solution with a 5-minute recovery point objective (RPO).

Which option will best fulfill the needs of the business?

- A. Configure AWS Backup to perform cross-Region backups of all servers every 5 minutes. Reprovision the three tiers in the DR Region from the backups using AWS CloudFormation in the event of a disaster.
- B. Maintain another running copy of the web and application server stack in the DR Region using AWS CloudFormation drift detection. Configure cross-Region snapshots of the DB instance to the DR Region every 5 minutes. In the event of a disaster, restore the DB instance using the snapshot in the DR Region.
- C. Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Regions. Create a cross-Region read replica of the DB instance in the DR Region. In the event of a disaster, promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIs.
- D. Create AMIs of the web and application servers in the DR Region. Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region. In the event of a disaster, switch to the DB instance in the DR Region and reprovision the servers with AWS CloudFormation using the AMIs.

Commented [LC352]: C
It can't be A becasue cross-Region backup of a large RDS MySQL could take more than 5 minutes and in fact often takes 1+ hrs. This is done with a copy and not a continuous replication. So a backup job would not complete fast enough to be able to meet the 5 min RPO.

Question #680

You've created your first Lambda function and want to monitor it using Cloudwatch metrics.

Cloudwatch can monitor which of the following Lambda metrics?

- 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

Commented [LC353]: AWS Lambda automatically monitors functions on your behalf, reporting metrics through Amazon CloudWatch (CloudWatch). These metrics include total invocations, errors, duration, and throttles.
Reference:
http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-metrics.html

Question #681

Determine the right expiry date for the "Letter of Authorization and Connecting Facility Assignment (LOA-CFA),"

which enables you to complete the Cross Connect stage of AWS Direct Connect configuration.

- A. If the cross connect is not completed within 90 days, the authority granted by the LOA-CFA expires.
- B. If the virtual interface is not created within 72 days, the LOA-CFA becomes outdated.
- C. If the cross connect is not completed within a user-defined time, the authority granted by the LOA- CFA expires.
- D. If the cross connect is not completed within the specified duration from the appropriate provider, the LOA-CFA expires.

Commented [LC354]: An AWS Direct Connect location provides access to AWS in the region it is associated with. You can establish connections with AWS Direct Connect locations in multiple regions, but a connection in one region does not provide connectivity to other regions.

Note: If the cross connect is not completed within 90 days, the authority granted by the LOA-CFA expires.

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

Question #682

A business just launched a new application on a cluster of Amazon EC2 Linux instances contained inside a VPC. The organization created an EC2 Linux instance as a bastion host in a peering VPC. The application instances' security group restricts access to TCP port 22 from the bastion host's private IP address. The bastion host's security group permits access to TCP port 22 from 0.0.0.0/0, allowing system administrators to remotely connect in to application instances through SSH from several branch offices.
While poring through the bastion host's operating system logs, a cloud engineer detects hundreds of unsuccessful SSH login attempts from places all over the globe. The cloud engineer wants to modify the way remote access to application instances is given and wishes to adhere to the following requirements:
⇨ Eliminate brute-force SSH login attempts.
⇨ Retain a log of commands run during an SSH session.
⇨ Retain the ability to forward ports.

Which solution satisfies these remote access criteria for application instances?

- A. Configure the application instances to communicate with AWS Systems Manager. Grant access to the system administrators to use Session Manager to establish a session with the application instances. Terminate the bastion host.
- B. Update the security group of the bastion host to allow traffic from only the public IP addresses of the branch offices.
- C. Configure an AWS Client VPN endpoint and provision each system administrator with a certificate to establish a VPN connection to the application VPC. Update the security group of the application instances to allow traffic from only the Client VPN IPv4 CIDR. Terminate the bastion host.
- D. Configure the application instances to communicate with AWS Systems Manager. Grant access to the system administrators to issue commands to the application instances by using Systems Manager Run Command. Terminate the bastion host.

Commented [LC355]: A.
"Session Manager removes the need to open inbound ports, manage SSH keys, or use bastion hosts"
Ref: https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

Port forwarding is supported:
https://aws.amazon.com/blogs/aws/new-port-forwarding-using-aws-system-manager-sessions-manager/

Question #683

A business is managing thousands of Amazon EC2 instances with the help of an existing orchestration technology. A recent penetration test discovered a weakness in the software stack of the organization. This risk led the organization to conduct a comprehensive assessment of its present manufacturing environment. According to the investigation, the following vulnerabilities exist in the environment:

⇨ Operating systems with outdated libraries and known vulnerabilities are being used in production.
⇨ Relational databases hosted and managed by the company are running unsupported versions with known vulnerabilities.
⇨ Data stored in databases is not encrypted.

The solutions architect aims to utilize AWS Config to regularly audit and analyze compliance with the company's rules and standards for AWS resource settings.

What additional measures will allow the business to protect its surroundings and manage its resources while adhering to best practices?

- A. Use AWS Application Discovery Service to evaluate all running EC2 instances. Use the AWS CLI to modify each instance, and use EC2 user data to install the AWS Systems Manager Agent during boot. Schedule patching to run as a Systems Manager Maintenance Windows task. Migrate all relational databases to Amazon RDS and enable AWS KMS encryption.
- B. Create an AWS CloudFormation template for the EC2 instances. Use EC2 user data in the CloudFormation template to install the AWS Systems Manager Agent, and enable AWS KMS encryption on all Amazon EBS volumes. Have CloudFormation replace all running instances. Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to execute AWS-RunPatchBaseline using the patch baseline.
- C. Install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool. Use the Systems Manager Run Command to execute a list of commands to upgrade software on each instance using operating system-specific tools. Enable AWS KMS encryption on all Amazon EBS volumes.
- D. Install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool. Migrate all relational databases to Amazon RDS and enable AWS KMS encryption. Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to execute AWS-RunPatchBaseline using the patch baseline.

Commented [LC356]: B, C -eliminated, no mention of RDS A - AWS Application Discovery Service involved with on premise migration, so eliminate it.

Question #684

A solutions architect is assessing the dependability of a freshly transferred application running on Amazon Web Services. Amazon S3 is used to host the front end, which is expedited through Amazon CloudFront. The application layer is implemented as a stateless Docker container running on an Amazon EC2 On-Demand Instance with an Elastic IP address. The storage layer is a MongoDB database operating in the same Availability Zone as the application layer on an EC2 Reserved Instance.

Which sequence of actions should the solutions architect do to reduce single points of failure while requiring minimum modifications to the application's code? (Select two.)

- A. Create a REST API in Amazon API Gateway and use AWS Lambda functions as the application layer
- B. Create an Application Load Balancer and migrate the Docker container to AWS Fargate
- C. Migrate the storage layer to Amazon DynamoDB
- D. Migrate the storage layer to Amazon DocumentDB (with MongoDB compatibility)
- E. Create an Application Load Balancer and move the storage layer to an EC2 Auto Scaling group

Commented [LC357]: I'll go with B,D

https://aws.amazon.com/documentdb/?nc1=h_ls

https://aws.amazon.com/blogs/containers/using-alb-ingress-controller-with-amazon-eks-on-fargate/

Commented [LC358]:

Question #685

A business wishes to relocate its website from an on-premises data center to Amazon Web Services (AWS). Simultaneously, it wishes to transition the website to a containerized microservices architecture in order to increase availability and cost effectiveness. According to the company's security policy, privileges and network permissions must be established in accordance with best practices, with the least privilege possible.
A Solutions Architect must design a containerized architecture that adheres to the application's security criteria and has deployed it on an Amazon ECS cluster.

What procedures are necessary upon deployment to ensure compliance with the requirements? (Select two.)

- A. Create tasks using the bridge network mode.
- B. Create tasks using the awsvpc network mode.
- C. Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.
- D. Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources.
- E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

Commented [LC359]: I would go for B, E.

https://amazonaws-china.com/blogs/compute/introducing-cloud-native-networking-for-ecs-containers/

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html

With the default bridge network mode, containers on an instance are connected to each other using the docker0 bridge.

This means you cannot address these containers with the IP address allocated by Docker (it's allocated from a pool of locally scoped addresses), nor can you enforce finely grained network ACLs and firewall rules. Instead, containers are addressable in your VPC by the combination of the IP address of the primary elastic network interface of the instance, and the host port to which they are mapped (either via static or dynamic port mapping). Also, because a single elastic network interface is shared by multiple containers, it can be difficult to create easily understandable network policies for each container.

The awsvpc networking mode addresses these issues by provisioning elastic network interfaces on a per-task basis. Hence, containers no longer share or contend use these resources.

Question #686 (SKIP)

Your department generates frequent analytics reports from the log files of your business. All log data is stored in Amazon S3 and processed daily by Amazon Elastic MapReduce (EMR) operations that produce daily PDF reports and aggregated CSV tables for an Amazon Redshift data warehouse.
Your CFO demands that you improve this system's cost structure.

Which of the following choices will reduce expenses without jeopardizing the system's average performance or the raw data's integrity?

- 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.

Commented [LC360]:

Commented [LC361]: C
First of all, this question is outdated, since as of 2020, RRS is not one of the available object classes for S3. So, this question will never come in certification exam.

https://aws.amazon.com/ec2/spot/use-case/emr/

provides an use case for EC2 sport instances "Amazon EMR on EC2 Spot Instances". Due to the fault-tolerant nature of big data workloads on EMR, they can continue processing, even when interrupted. Running EMR on Spot Instances drastically reduces the cost of big data, allows for significantly higher compute capacity, and reduces the time to process big data sets. Also, if Raw data is available all processing can be redone.

Question #687

The Principal element of an IAM policy denotes the particular entity to whom authorization should be granted or denied, while the ____ denotes everyone except the specified entity.

- A. NotPrincipal
- B. Vendor
- C. Principal
- D. Action

Commented [LC362]: Use the NotPrincipal element to specify the IAM user, federated user, IAM role, AWS account, AWS service, or other principal that is not allowed or denied access to a resource. The NotPrincipal element enables you to specify an exception to a list of principals. Use this element to deny access to all principals except the one named in the NotPrincipal element. The syntax for specifying NotPrincipal is the same as for specifying AWS JSON policy elements: Principal.

You cannot use the NotPrincipal element in an IAM identity-based policy. You can use it in the trust policies for IAM roles and in resource-based policies. Resource-based policies are policies that you embed directly in an IAM resource.

Question #688

A business has a data center that must be swiftly moved to AWS. The data center is connected to Amazon Web Services through a 500 Mbps AWS Direct Connect connection and a separate, fully accessible 1 Gbps ISP connection. A Solutions Architect is tasked with the responsibility of transferring 20 terabytes of data from the data center to an Amazon S3 bucket.

What is the FASTEST method of data transfer?

- 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.

Commented [LC363]: Transfer Acceleration over a fully available 1 Gbps can theoretically move around 10TB/Day.

1 Gbps = (1024/8) MBPs = 128 MBps
(128 MBps * 3600 secs * 24 Hrs)/1024 = 10,800 GB/Day = 10TB/Day

Along with Transfer Acceleration, which provides a consistent experience, the entire data can be moved in 2 days. However, AWS Import/Export (now snowball) takes around a week to make the data available on AWS. The Answer is D.

Question #689

What is the maximum write throughput that a single Dynamo DB table can support?

- A. 1,000 write capacity units
- B. 100,000 write capacity units
- C. Dynamo 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

Commented [LC364]: It looks like an outdated question. It is now 40000 by default

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Limits.html#default-limits-throughput-capacity-modes

Question #690

You've added a new instance to your Auto Scaling group, which is now subject to ELB health checks. A health check performed by the ELB indicates that the new instance's status is out of service.

What role does Auto Scaling play in this scenario?

- A. It replaces the instance with a healthy one
- B. It stops the instance
- C. It marks an instance as unhealthy
- D. It terminates the instance

Commented [LC365]:

Question #691

ABC developed a multi-tenant Learning Management System (LMS). The application is hosted for five distinct tenants (customers) in VPCs associated with each tenant's AWS account. ABC want to establish a centralized server that can communicate with the LMS of each tenant and perform necessary upgrades. Additionally, ABC want to guarantee that one tenant VPC is unable to communicate with the other tenant VPC for security concerns.

How is ABC going to put up this scenario?

- A. ABC has to setup one centralized VPC which will peer in to all the other VPCs of the tenants.
- B. ABC should setup VPC peering with all the VPCs peering each other but block the IPs from CIDR of the tenant VPCs to deny them.
- C. ABC should setup all the VPCs with the same CIDR but have a centralized VPC. This way only the centralized VPC can talk to the other VPCs using VPC peering.
- D. ABC should setup all the VPCs meshed together with VPC peering for all VPCs.

Commented [LC366]: A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. A VPC peering connection allows the user to route traffic between the peer VPCs using private IP addresses as if they are a part of the same network.
This is helpful when one VPC from the same or different AWS account wants to connect with resources of the other VPC. The organization wants to setup that one VPC can connect with all the other VPCs but all other VPCs cannot connect among each other. This can be achieved by configuring VPC peering where one
VPC is peered with all the other VPCs, but the other VPCs are not peered to each other. The VPCs are in the same or a separate AWS account and should not have overlapping CIDR blocks.

Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html#many-vpcs-full-acces

Question #692

A team gathers and distributes behavioral data throughout an organization. The organization operates a Multi-AZ VPC environment with public and private subnets, as well as an internet gateway. Additionally, each public subnet incorporates a NAT gateway. The majority of the company's applications read and write data to and from Amazon Kinesis Data Streams.
The majority of workloads are conducted in private subnets.
A solutions architect must do an assessment of the infrastructure. The solution architect must minimize expenses while maintaining the apps' functionality. Cost Explorer is used by the solutions architect to determine that the cost in the EC2-Other category is continuously high. A further investigation reveals that the NatGateway-Bytes charges are raising the cost of EC2-Other.

What actions should the solutions architect take to ensure that these criteria are met?

- A. Enable VPC Flow Logs. Use Amazon Athena to analyze the logs for traffic that can be removed. Ensure that security groups are blocking traffic that is responsible for high costs.
- B. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that applications have the correct IAM permissions to use the interface VPC endpoint.
- C. Enable VPC Flow Logs and Amazon Detective. Review Detective findings for traffic that is not related to Kinesis Data Streams. Configure security groups to block that traffic.
- D. Add an interface VPC endpoint for Kinesis Data Streams to the VPC. Ensure that the VPC endpoint policy allows traffic from the applications.

Commented [LC367]: D: If most traffic through your NAT gateway is to AWS services that support interface VPC endpoints, then create an interface VPC endpoint for the services.

https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/

VPC endpoint policies enable you to control access by either attaching a policy to a VPC endpoint or by using additional fields in a policy that is attached to an IAM user, group, or role to restrict access to only occur via the specified VPC endpoint

Question #693

AWS CloudFormation _____ are template-specific actions that you use to set values to attributes that are not accessible until runtime.

- A. intrinsic functions
- B. properties declarations
- C. output functions
- D. conditions declarations

Commented [LC368]: AWS CloudFormation intrinsic functions are special actions you use in your template to assign values to properties not available until runtime. Each function is declared with a name enclosed in quotation marks (""), a single colon, and its parameters.

Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-fuctions-structure.html

Question #694

Which Amazon Web Services instance address has the following characteristics? "When an instance is stopped, its Elastic IP address becomes unmapped, which must be remapped when the instance is restarted."

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

Commented [LC369]: Stopping an instance -

EC2-Classic -
If you stop an instance, its Elastic IP address is disassociated, and you must reassociate the Elastic IP address when you restart the instance.

EC2-VPC -
If you stop an instance, its Elastic IP address remains associated.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

Question #695

A user intends to utilize EBS to meet his database requirements. The user already has an Amazon Elastic Compute Cloud (EC2) instance operating in the VPC private subnet.

How can a user connect an EBS volume to an already-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.

Commented [LC370]: 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.

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

Question #696

A Solutions Architect is tasked with the responsibility of migrating a legacy application from on-premises to AWS. On-premises, the application runs on two Linux servers protected by a load balancer and connects to a master-master database spread over two servers. Each application server needs a license file that is associated with the server's network adapter's MAC address. The software provider needs 12 hours to give ne licensing files through email. To utilize static, the program needs configuration files. IPv4 addresses, not DNS, are used to connect to database servers.

Which measures, in combination with the others, should be completed to provide a scalable architecture for the application servers? (Select two.)

- A. Create a pool of ENIs, request license files from the vendor for the pool, and store the license files within Amazon S3. Create automation to download an unused license, and attach the corresponding ENI at boot time.
- B. Create a pool of ENIs, request license files from the vendor for the pool, store the license files on an Amazon EC2 instance, modify the configuration files, and create an AMI from the instance. use this AMI for all instances.
- C. Create a bootstrap automation to request a new license file from the vendor with a unique return email. Have the server configure itself with the received license file.
- D. Create bootstrap automation to attach an ENI from the pool, read the database IP addresses from AWS Systems Manager Parameter Store, and inject those parameters into the local configuration files. Keep SSM up to date using a Lambda function.
- E. Install the application on an EC2 instance, configure the application, and configure the IP address information. Create an AMI from this instance and use if for all instances.

Commented [LC371]:

Commented [LC372]:

Question #697

You are developing a solution to prevent data leakage in your VPC environment. You want your VPC Instances to be able to connect to online software repositories and distributions for product updates. By their URLs, the depots and distributions are available via third-party CDNs.
You wish to expressly prevent any more outbound connections from your VPC instances to external hosts.

Which of the following are you considering?

- 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.

Commented [LC373]: Answer is A.

B: SG is for allow only.
D: NACL is for deny and allow but cannot only via IP or Port. Cannot deny url.
C: where is the NAT?

Question #698

An architect has deployed an operational workload on Amazon EC2 instances in an Auto Scaling group. The VPC design spans two Availability Zones (AZ), each with a dedicated subnet for the Auto Scaling group. The VPC is physically attached to an on-premises environment and cannot be disconnected. The Auto Scaling group may have a maximum of 20 instances in service. The IPv4 addressing scheme for the VPC is as follows:

VPC CIDR: 10.0.0.0/23
AZ1 subnet CIDR: 10.0.0.0/24
AZ2 subnet CIDR: 10.0.1.0/24

Since deployment, the Region has gained access to a third AZ. The solutions architect wants to implement the new AZ without expanding IPv4 address space or causing service outage.

Which solution will satisfy these criteria?

- A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space. Adjust the Auto Scaling group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.
- B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
- C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.
- D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.

Commented [LC374]: A
---
https://aws.amazon.com/premiumsupport/knowledge-center/vpc-ip-address-range/?nc1=h_ls
It's not possible to modify the IP address range of an existing virtual private cloud (VPC) or subnet. You must delete the VPC or subnet, and then create a new VPC or subnet with your preferred CIDR block.

A, no downtime, D is incorrect as CIDR can't be updated in this case.

Question #699

A solutions architect at a big organization is responsible for configuring network security for outgoing traffic to the internet from all AWS accounts inside the corporation's AWS Organizations. The business has over 100 AWS accounts, which are connected through a centralized AWS Transit Gateway. Each account is equipped with both an internet gateway and a NAT gateway for outgoing internet traffic. The organization limits its AWS resource deployments to a single AWS Region.
The business needs the ability to implement centrally controlled rule-based filtering to all outgoing traffic to the internet for all AWS accounts. In each Availability Zone, the peak load of outbound traffic will not exceed 25 Gbps.

Which solution satisfies these criteria?

- A. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Create an Auto Scaling group of Amazon EC2 instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region. Modify all default routes to point to the proxy's Auto Scaling group.
- B. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Use an AWS Network Firewall firewall for rule-based filtering. Create Network Firewall endpoints in each Availability Zone. Modify all default routes to point to the Network Firewall endpoints.
- C. Create an AWS Network Firewall firewall for rule-based filtering in each AWS account. Modify all default routes to point to the Network Firewall firewalls in each account.
- D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering. Modify all default routes to point to the proxy's Auto Scaling group.

Commented [LC375]: B
Source: https://aws.amazon.com/blogs/networking-and-content-delivery/deployment-models-for-aws-network-firewall/

Questions 700-799

Question #700

A business may have many AWS accounts and administers them using AWS Organizations. A developer was provided with IAM user credentials in order to get access to AWS resources. The developer should have read-only access to the account's Amazon S3 buckets. When the developer attempts to access the S3 buckets through the console, he or she receives an access denied error message with no bucket named.
After reviewing the permissions, the solution architect discovers that the developer's IAM user is marked as having read-only access to all S3 buckets in the account.

Which extra troubleshooting actions should the solutions architect take? (Select two.)

- A. Check the bucket policies for all S3 buckets.
- B. Check the ACLs for all S3 buckets.
- C. Check the SCPs set at the organizational units (OUs).
- D. Check for the permissions boundaries set for the IAM user.
- E. Check if an appropriate IAM role is attached to the IAM user.

Commented [LC376]: Answer C and D
- My two cents:
A is INCORRECT even though a bucket policy IS a resource based policy and will be evaluated AFTER Organizations SCPs, if a DENY is set in the policy you will list see it listed. You will see the word "ERROR" in the Access column.

B is INCORRECT because even though ACLs are resource-based policies you use ACLs to grant basic read/write permissions on the objects in the bucket. You'll still be able to ListBuckets if there is an ACL on the bucket.

C is CORRECT because after the Deny Evaluation a Organization SCPs are evaluated and take affect/merged. (See Link Below)

D is CORRECT because a DENY on the permission boundary will not allow the developer to ListBuckets

E is INCORRECT because this is a IAM Permission and applied AFTER DENY, ORG SCP, and RESOURCE-based policy evaluation. In addition, the Solution Architect checked the developers IAM User and it was listed as readonly.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow

note: to understand better permission boundary check the following ref:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Question #701

Recently, a company's CFO evaluated the company's monthly AWS bill and saw an opportunity to minimize the cost of the company's AWS Elastic Beanstalk instances in use. The CFO has tasked a Solutions Architect with designing a highly available solution that would automatically fire up an Elastic Beanstalk environment in the morning and shut it down at the end of the day.
The solution should be created with the least amount of operational overhead and the lowest possible cost. Additionally, it should be able to manage the rising usage of Elastic Beanstalk instances by various teams and offer a centralized scheduling solution for all teams to keep operating expenses low.

Which design will satisfy these criteria?

- A. Set up a Linux EC2 Micro instance. Configure an IAM role to allow the start and stop of the Elastic Beanstalk environment and attach it to the instance. Create scripts on the instance to start and stop the Elastic Beanstalk environment. Configure cron jobs on the instance to execute the scripts.
- B. Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution role granting Elastic Beanstalk environment start/stop permissions, and assign the role to the Lambda functions. Configure cron expression Amazon CloudWatch Events rules to trigger the Lambda functions.
- C. Develop an AWS Step Functions state machine with 'wait' as its type to control the start and stop time. Use the activity task to start and stop the Elastic Beanstalk environment. Create a role for Step Functions to allow it to start and stop the Elastic Beanstalk environment. Invoke Step Functions daily.
- D. Configure a time-based Auto Scaling group. In the morning, have the Auto Scaling group scale up an Amazon EC2 instance and put the Elastic Beanstalk environment start command in the EC2 instance user data. At the end of the day, scale down the instance number to 0 to terminate the EC2 instance.

Commented [LC377]:

Commented [LC378]: B
https://aws.amazon.com/premiumsupport/knowledge-center/schedule-elastic-beanstalk-stop-restart/

Question #702

A business wishes to develop a serverless application utilizing Amazon API Gateway, Amazon Lambda, and Amazon DynamoDB. They demonstrated the idea and said that the average response time exceeds the tolerances of their upstream services. Amazon CloudWatch measurements revealed no problems with DynamoDB, but did suggest that certain Lambda operations had reached their timeout.

Which of the following should the Solutions Architect consider while optimizing performance? (Select 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.

Commented [LC379]: BD
https://lumigo.io/blog/aws-lambda-timeout-best-practices/
A: While this will improve the situation, it may not be enough.
B: Memory – The amount of memory available to the function during execution. Choose an amount between 128 MB and 3,008 MB in 64 MB increments. Lambda allocates CPU power linearly in proportion to the amount of memory configured. At 1,792 MB, a function has the equivalent of 1 full vCPU (one vCPU-second of credits per second).
All calls made to AWS Lambda must complete execution within 900 seconds. The default timeout is 3 seconds, but you can set the timeout to any value between 1 and 900 seconds.
C: The problem is not with the DB.
D: AWS API Gateway has a max timeout of 29 seconds for all integration types, which includes Lambda as well. It means that any API call coming through API Gateway cannot exceed 29 seconds. It makes sense for most of the APIs except for few high computational ones.
E: Increase the memory not CPU.

Question #703

A financial services organization maintains an on-premises system that consumes market data feeds from stock exchanges, processes the data, and distributes it to an internal Apache Kafka cluster. Management wants to utilize AWS services in order to develop a scalable and near-real-time solution capable of delivering stock market data to a web application in a consistent manner.

Which stages should a solutions architect follow while developing a solution? (Select three.)

- A. Establish an AWS Direct Connect connection from the on-premises data center to AWS.
- B. Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Consumer Library to put the data into an Amazon Kinesis data stream.
- C. Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Kinesis Producer Library to put the data into a Kinesis data stream.
- D. Create a WebSocket API in Amazon API Gateway, create an AWS Lambda function to process an Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.
- E. Create a GraphQL API in AWS AppSync, create an AWS Lambda function to process the Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.
- F. Establish a Site-to-Site VPN from the on-premises data center to AWS.

Commented [LC380]:

Commented [LC381]: ACD. Direct Connect to ensure reliable network connection between on premise to VPC, transfer Kafka content into Kinese Data Stream and then use websocket to connect to web application clients.

Commented [LC382]:

Commented [LC383]:

Question #704

To comply with industry laws, a Solutions Architect must create a solution that securely stores a business's important data across various public AWS Regions, including the United States, where the business's headquarters are situated. The Solutions Architect is responsible for ensuring that the data stored in AWS is accessible over the company's worldwide WAN network. The security team has mandated that no traffic requesting access to this data be sent over the public internet.

How should the Solutions Architect develop a highly accessible, cost-effective solution that satisfies the requirements?

- A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
- B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
- C. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
- D. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.

Commented [LC384]: This feature also allows you to connect to any of the participating VPCs from any Direct Connect location, further reducing your costs for making using AWS services on a cross-region basis.
https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/
A: There is only a single DC and hence is not highly available.
B: VPC peering means there are additional cost charges when data transfer between region. Also there is a 125 VPC peering limit. Data transferred across Inter-Region VPC Peering connections is charged at the standard inter-region data transfer rates. https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/
C: Similar to B.
D: Remember one caveat which the question did not state is if there are multiple accounts: The VPCs that reference a particular Direct Connect Gateway must have IP address ranges that do not overlap. Today, the VPCs must all be in the same AWS account; will make this more flexible in the future. https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/

Question #705

What is the suggested average queue length by AWS to obtain the lowest possible latency for the 200 PIOPS EBS volume?

- A. 5
- B. 1
- C. 2
- D. 4

Commented [LC385]: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/benchmark_procedures.html#UnderstandingQueueLength

For PIOPS, queue length is 1 for every 1000 IOPS

Question #706

You're operating an application on an EC2 instance that enables customers to download files from a private S3 bucket using a pre-signed URL. Prior to establishing the URL, the application should ensure that the file exists in S3.

How should the application safely access the S3 bucket using AWS credentials?

- 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.

Commented [LC386]: Duplicated question.

C is the right answer.

Question #707

Which of the following statements about the DynamoDB Console is NOT true?

- 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 table, add, update, and delete items.

Commented [LC387]: 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.

LSI can't be created after the table's creation.

Question #708

How many metrics does CloudWatch provide for Auto Scaling?

- A. 7 metrics and 5 dimensions
- B. 5 metrics and 1 dimension
- C. 1 metric and 5 dimensions
- D. 8 metrics and 1 dimension

Commented [LC388]: D
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-monitoring.html

GroupMinSize
GroupMaxSize
GroupDesiredCapacity
GroupInServiceInstances
GroupPendingInstances
GroupStandbyInstances
GroupTerminatingInstances
GroupTotalInstances

Question #709

A public retail web application utilizes an Application Load Balancer (ALB) in front of Amazon EC2 instances distributed across different Availability Zones (AZs) within a Region that is powered by an Amazon RDS MySQL Multi-AZ deployment. The health checks for the target group are set to utilize HTTP and refer to the product catalog page. Auto Scaling is designed to maintain the size of the web fleet in accordance with the results of the ALB health check.
Recently, the application was unavailable. Throughout the downtime, Auto Scaling constantly replaced the instances. Following an inspection, it was revealed that although the web server metrics were within normal range, the database tier was under heavy stress, resulting in significantly increased query response times.

Which of the following adjustments would resolve these concerns while also increasing monitoring capabilities for the whole application stack's availability and functioning in preparation for future growth? (Select 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.

Commented [LC389]: B E

A: Since the issue lies with query response (read) it is cheaper and faster to use ElastiCache which is in memory. The problem in A is that "reader endpoint" is for Aurora, not RDS!

D: Should not recover the RDS instance.

Commented [LC390]:

Question #710

Your firm creates one-of-a-kind skiing helmets on commission from customers, fusing high fashion with specific technological advancements. Customers may flaunt their Individuality on the ski slopes, thanks to the availability of head-up displays. GPS rearview cameras and any other technological advancements they desire to include into the helmet.
The present production process is data-intensive and sophisticated, requiring evaluations to guarantee that the bespoke electronics and materials used to construct the helmets meet the highest requirements. Assessments are a combination of manual and computerized evaluations. You must add a new set of assessments to simulate the failure modes of the bespoke electronics utilizing GPUs and CUDA, distributed over a cluster of servers with low-latency networking.

Which architecture would enable you to automate an existing process using a hybrid approach while also ensuring that the architecture is capable of supporting process change over time?

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

Commented [LC391]: B.
I think both data pipeline and swf work.
But data pipeline focuses on creation and management of periodic batch-processing data-driven workloads, particularly ones using AWS storage services.
So swf is a better fit here.

Question #711

A newspaper organization maintains an on-premises application that enables the public to search for and obtain specific newspaper pages through a Java-based website. They scanned the old newspapers into JPEG files (about 17TB) and used Optical Character Recognition (OCR) to feed a commercial search engine. The hosting infrastructure and software are no longer supported, and the business want to transition its archive to AWS in order to create a cost-effective architecture while maintaining availability and durability.

Which is the most suitable?

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

Commented [LC392]: Answer is C
A. Use S3 with RRS: RRS is not high availability
B. An EC2 instance and stripe multiple standard EBS volumes together: Not HA too
D. Use a single-AZ RDS MySQL: Not HA also RDS is not using for store image
E. Use a CloudFront: Missing CloudFront origin. Also using an EC2 will not HA

"... and the software are no longer supported" rules out A, E.

Question #712

On Amazon EC2, a web startup hosts its very successful social news service using an Elastic Load Balancer, an Auto-Scaling group of Java/Tomcat application servers, and DynamoDB as the data store. The primary web application performs optimally on m2xbig instances because to its high memory requirements. Each new deployment necessitates the semi-automated building and testing of a new AMI for the application servers, which takes a considerable amount of time and is consequently only performed once per week.
Recently, a new chat functionality was introduced into the architecture using nodejs and wails. The first testing indicate that the new component is CPU-bound. Due to the company's prior experience with Chef, they chose to streamline the deployment process by using AWS Ops Works as an application life cycle management platform to simplify application administration and minimize deployment cycles.

What AWS Ops Works setup is required to incorporate the new chat module in the most cost-effective and flexible manner possible?

- 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 recipes

Commented [LC393]: B
http://jayendrapatil.com/category/aws/opsworks/

Create one AWS Ops Works stack, create two AWS Ops Works layers create one custom recipe (Single environment stack, two layers for java and node.js application using built-in recipes and custom recipe for DynamoDB connectivity only as other configuration. Refer link)

Question #713

A financial institution is running its mission-critical application on Amazon Web Services' current-generation Linux EC2 instances. The program features a self-managed MySQL database that handles a large amount of I/O. The application is doing well in terms of handling a reasonable quantity of traffic throughout the month. However, it slows down significantly during the last three days of each month owing to month-end reporting, despite the fact that the firm uses Elastic Load Balancers and Auto Scaling to meet increasing demand.

Which of the following actions would enable the database to manage the month-end load with the LEAST amount of performance degradation?

- A. Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.
- B. Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.
- C. Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.
- D. Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

Commented [LC394]: C is the right answer.

Spiking Demand – You are running a relational database on a Provisioned IOPS volume that is set to handle a moderate amount of traffic during the month, with a 10x spike in traffic during the final three days of each month due to month-end processing. You can use Elastic Volumes to dial up the provisioning in order to handle the spike, and then dial it down afterward.

Anyone who thinks "B" has the LEAST IMPACT on performance has clearly never migrated a database between platforms before, although I agree it will provide the greatest long-term performance and is in alignment with AWS recognized success patterns. Database migration for PRODUCTION databases that are needed every day for reporting isn't a small job--for a large company with many departments this effort could take several months and completely bog down the Database staff. "C" is an option with virtually zero impact on day-to-day performance and can be entirely managed by the Cloud Architect. Read carefully.

https://aws.amazon.com/blogs/aws/amazon-ebs-update-new-elastic-volumes-change-everything/

Question #714

A significant mobile gaming firm just completed a successful migration of its on-premises infrastructure to the AWS Cloud. A solutions architect is doing an assessment of the environment to confirm that it was constructed in accordance with the design and is operating in accordance with the Well-Architected Framework.

While analyzing prior monthly charges in Cost Explorer, the solutions architect finds that the creation and subsequent termination of various big instance types use a disproportionate amount of resources. The solutions architect discovers that the company's developers are creating new Amazon EC2 instances for testing purposes and are not utilizing the correct instance types.

The solutions architect must design a method that restricts the instance kinds that may be launched by only developers.

Which solution will satisfy these criteria?

- A. Create a desired-instance-type managed rule in AWS Config. Configure the rule with the instance types that are allowed. Attach the rule to an event to run each time a new EC2 instance is launched.
- B. In the EC2 console, create a launch template that specifies the instance types that are allowed. Assign the launch template to the developers' IAM accounts.
- C. Create a new IAM policy. Specify the instance types that are allowed. Attach the policy to an IAM group that contains the IAM accounts for the developers.
- D. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

Commented [LC395]: B, D wrong.

A may be right, but C is correct.

An example policy to attach to the group:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "overrideBlockOnReq",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "ARN-OF-ROLE"
    },
    {
      "Sid": "limitedSize",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "ForAnyValue:StringNotLike": {
          "ec2:InstanceType": [
            "*.nano",
            "*.small",
            "*.micro",
            "*.medium"
          ]
        }
      }
    }
  ]
```

... [2]

Question #715

A user wishes to run both a web server and an application server on a single EC2 instance that is part of a VPC's public subnet.

How can the user configure two distinct public IP addresses and security groups for the application and 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.

Commented [LC396]: 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.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html

Question #716

A business operates its AWS infrastructure in two AWS Regions. The firm operates four virtual private clouds in the eu-west-1 region and two in the us-east-1 region. Additionally, the firm has an on-premises data center in Europe, which is connected to AWS through two AWS Direct Connect connections in eu-west-1.
The organization requires a solution that enables Amazon EC2 instances inside each VPC to communicate with one another using private IP addresses. Additionally, servers in the on-premises data center must be able to access those VPCs through private IP addresses.

Which approach is the MOST cost-effective in terms of meeting these requirements?

- A. Create an AWS Transit Gateway in each Region, and attach each VPC to the transit gateway in that Region. Create cross-Region peering between the transit gateways. Create two transit VIFs, and attach them to a single Direct Connect gateway. Associate each transit gateway with the Direct Connect gateway.
- B. Create VPC peering between each VPC in the same Region. Create cross-Region peering between each VPC in different Regions. Create two private VIFs, and attach them to a single Direct Connect gateway. Associate each VPC with the Direct Connect gateway.
- C. Create VPC peering between each VPC in the same Region. Create cross-Region peering between each VPC in different Regions. Create two public VIFs that are configured to route AWS IP addresses globally to on-premises servers.
- D. Create an AWS Transit Gateway in each Region, and attach each VPC to the transit gateway in that Region. Create cross-Region peering between the transit gateways. Create two private VIFs, and attach them to a single Direct Connect gateway. Associate each VPC with the Direct Connect gateway.

Commented [LC397]: The focus here is to be cost efficient.

A - In correct. It will work, but there is cost for each transit gateway

B - Correct.
https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-gateway-vs-vpc-peering.html
"Lower cost — With VPC peering you only pay for data transfer charges. Transit Gateway has an hourly charge per attachment in addition to the data transfer fees. "

C - public VIFs is for public IP

D - for transit gateways, you need transit VIFs, not private VIFs.

Question #717 (SKIP)

AWS Direct Connect does not include any resources to which you may restrict access. As a result, you will not be able to utilize AWS Direct Connect Amazon Resource Names (ARNs) in an Identity and Access Management (IAM) policy.

With this in mind, how can a policy be written to restrict 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.

Question #718 (SKIP)

How many cg1.4xlarge on-demand instances can a user operate in a single region without obtaining AWS clearance for a limit increase?

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

Question #719

A firm is using Elastic Beanstalk to create a highly scalable application.
Elastic Load Balancing (ELB) and a Virtual Private Cloud (VPC) with public and private subnets are being used. They must meet the following criteria:
- All the EC2 instances should have a private IP
- All the EC2 instances should receive data via the ELB's.

Which of these will be unnecessary in this configuration?

- 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.

Question #720

Which of the following assertions is FALSE when interacting with your AWS Direct Connect connection once it has been fully configured?

- A. You can manage your AWS Direct Connect connections and view the connection details.
- B. You can delete a connection as long as there are no virtual interfaces attached to it.
- C. You cannot view the current connection ID and verify if it matches the connection ID on the Letter of Authorization (LOA).
- D. You can accept a host connection by purchasing a hosted connection from the partner (APN).

Commented [LC398]: QUESTION IS OLD, NOW THERE ARE ARNS

Answer is C
But now DirectConnect has provide ARNs
https://docs.aws.amazon.com/directconnect/latest/UserGuide/security_iam_service-with-iam.html

Commented [LC399]: OLD QUESTION, NOW IT'S NOT LIKE THIS.

The limit is based on vCPU. vCPU calculator can help calculating how many instances for each category.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html#ec2-on-demand-instances-limits https://aws.amazon.com/ec2/faqs/#EC2_On-Demand_Instance_limits

BEFORE IT WAS 2:

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.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_ec2

Commented [LC400]: CAREFUL, it says "UNNECESSARY" in the question.

The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web
Services (AWS) cloud. The user has complete control over the virtual networking environment. If the organization wants the Amazon EC2 instances to have a private IP address, he should create a public and private subnet for VPC in each Availability Zone (this is an AWS Elastic Beanstalk requirement). The organization should add their public resources, such as ELB and NAT to the public subnet, and AWC Elastic Beanstalk will assign them unique elastic IP addresses (a static, public IP address). The organization should launch Amazon EC2 instances in a private subnet so that AWS Elastic Beanstalk assigns them non-routable private IP addresses. Now the organization should configure route tables with the following rules:
⇨ route all inbound traffic from ELB to EC2 instances
⇨ route all outbound traffic from EC2 instances through NAT
Reference:

... [3]

Commented [LC401]: You can manage your AWS Direct Connect connections and view connection details, accept hosted connections, and delete connections. You can view the current status of your connection. You can also view your connection ID, which looks similar to this example dxcon-xxxx, and verify that it matches the connectionID on the Letter of Authorization (LOA) that you received from Amazon.

Reference:

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

Question #721

The public-facing WordPress site of a European online newspaper is hosted in a colocated data center in London. A load balancer, two web servers, and one MySQL database server comprise the current WordPress architecture. A solutions architect is assigned with the responsibility of building a solution that meets the following criteria:

⇨ Improve the website's performance
⇨ Make the web tier scalable and stateless
⇨ Improve the database server performance for read-heavy loads
⇨ Reduce latency for users across Europe and the US
⇨ Design the new architecture with a goal of 99.9% availability

Which method satisfies these criteria while improving operational efficiency?

- A. Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances in one AWS Region and three Availability Zones. Configure an Amazon ElastiCache cluster in front of a Multi-AZ Amazon Aurora MySQL DB cluster. Move the WordPress shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes the US and Europe.
- B. Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances in two AWS Regions and two Availability Zones in each Region. Configure an Amazon ElastiCache cluster in front of a global Amazon Aurora MySQL database. Move the WordPress shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes the US and Europe. Configure EFS cross-Region replication.
- C. Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances in one AWS Region and three Availability Zones. Configure an Amazon DocumentDB table in front of a Multi-AZ Amazon Aurora MySQL DB cluster. Move the WordPress shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes all global locations.
- D. Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances in two AWS Regions and three Availability Zones in each Region. Configure an Amazon ElastiCache cluster in front of a global Amazon Aurora MySQL database. Move the WordPress shared files to Amazon FSx with cross-Region synchronization. Configure Amazon CloudFront with the ALB as the origin and a price class that includes the US and Europe.

Commented [LC402]:

Question #722

Which of the following statements is true about temporary security credentials in IAM?

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

Commented [LC403]: Answer is A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_disable-perms.html

clearly mentioned Temporary security credentials are valid until they expire, and they cannot be revoked

but you can achieve the effect of revoking the credentials by changing the permissions for the credentials even after they have been issued its alternative way only.

Although, changing the permissions (so making the answer D valid) will revoke ALL credentials issued.

Badly written question.

Question #723

A solutions architect must design a multi-region architecture for an Amazon RDS for PostgreSQL database that will be used to support a web application. The database is launched using an AWS CloudFormation template that leverages AWS services and capabilities available in both the main and secondary regions.

The database is designed for automatic backups and has a recovery time objective (RTO) of 15 minutes and a recovery point objective (RPO) of 2 hours. The web application is set to send traffic to the database using an Amazon Route 53 record.

Which sequence of actions results in the most highly available architecture that satisfies all requirements? (Select two.)

- A. Create a cross-Region read replica of the database in the secondary Region. Configure an AWS Lambda function in the secondary Region to promote the read replica during failover event.
- B. In the primary Region, create a health check on the database that will invoke an AWS Lambda function when a failure is detected. Program the Lambda function to recreate the database from the latest database snapshot in the secondary Region and update the Route 53 host records for the database.
- C. Create an AWS Lambda function to copy the latest automated backup to the secondary Region every 2 hours.
- D. Create a failover routing policy in Route 53 for the database DNS record. Set the primary and secondary endpoints to the endpoints in each Region.
- E. Create a hot standby database in the secondary Region. Use an AWS Lambda function to restore the secondary database to the latest RDS automatic backup in the event that the primary database fails.

Commented [LC404]: It's possible to create a cross-region replica with RDS PostgreSQL

Commented [LC405]: Classic failover option with Route53

Question #724 (EXAM)

A business is launching a web-based application in many countries. The application has both static and dynamic content, which is stored in a private Amazon S3 bucket and hosted in Amazon ECS containers behind an Application Load Balancer (ALB). The organization stipulates that all static and dynamic application material must be available through Amazon CloudFront.

Which combination of procedures should a solutions architect propose to protect CloudFront's direct content access? (Select three.)

- A. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB.
- B. Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution.
- C. Configure CloudFront to add a custom header to origin requests.
- D. Configure the ALB to add a custom header to HTTP requests.
- E. Update the S3 bucket ACL to allow access from the CloudFront distribution only.
- F. Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution. Update the S3 bucket policy to allow access to the OAI only.

Commented [LC406]: The option that says: Use CloudFront to add a custom header to all origin requests. Using AWS WAF, create a web rule that denies all requests without this custom header.

Associate the web ACL to the CloudFront distribution is incorrect. If any new requests are going to CloudFront, they won't have the custom header initially so AWS WAF may block the request immediately.

This could deny any new connections to CloudFront. Therefore, you need to associate the web ACL to the ALB, which is after the CloudFront adds the custom header.

Commented [LC407]:

Commented [LC408]:

Question #725

Is the Amazon RDS API capable of modifying database instances inside a VPC and associating them with database 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.

Commented [LC409]: 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 #726

You're operating an application on an Amazon EC2 instance that enables users to download files from a private S3 bucket using a pre-signed URL. Prior to establishing the URL, the application should ensure that the file exists in S3.

How should the application safely access the S3 bucket using AWS credentials?

- 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.

Commented [LC410]: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

Question #727

What is the purpose of the PollForTask action when it is invoked by an AWS Data Pipeline task runner?

- A. It is used to retrieve the pipeline definition.
- B. It is used to report the progress of the task runner to AWS Data Pipeline.
- C. It is used to receive a task to perform from AWS Data Pipeline.
- D. It is used to inform AWS Data Pipeline of the outcome when the task runner completes a task.

Commented [LC411]: Task runners call PollForTask to receive a task to perform from AWS Data Pipeline. If tasks are ready in the work queue, PollForTask returns a response immediately. If no tasks are available in the queue, PollForTask uses long-polling and holds on to a poll connection for up to 90 seconds, during which time any newly scheduled tasks are handed to the task agent. Your remote worker should not call PollForTask again on the same worker group until it receives a response, and this may take up to 90 seconds.

Reference:
http://docs.aws.amazon.com/datapipeline/latest/APIReference/API_PollForTask.html

Question #728

A corporation generated accounts for each of its Development teams, totaling 200 accounts. Each account has a single virtual private cloud (VPC) in a single region, each of which has many microservices operating in Docker containers and requiring communication with microservices in other accounts. According to the Security team's needs, these microservices must not traverse the public internet, and only specific internal services should be permitted to contact other internal services. If any network traffic for a service is refused, the Security team must be alerted, including the originating IP.

How can connection between services be developed while adhering to 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.

Commented [LC412]: VPC Peering would be too much complicated. B doesn't make sense.

C 3rd party for Transit Gateway?

D is fine.

Question #729

You need the capacity to analyze massive volumes of data stored on Amazon S3 through Amazon Elastic Map Reduce. You're utilizing the EC2 8xlarge instance type, which has the majority of its CPUs idle during processing.

Which of the following would be the most cost-effective method of reducing the job's runtime?

- A. Create more, smaller files on Amazon S3.
- B. Add additional EC2 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.

Commented [LC413]: A, B are wrong.

D is tempting but C is correct

Question #730

Your organization now operates a two-tier web application from an on-premises data center. You've had many infrastructure failures during the last two months, resulting in substantial financial losses. Your CIO is adamant about moving the application to AWS. While he works to get buy-in from other corporate leaders, he wants you to prepare a disaster recovery plan to aid in short-term business continuity. He targets a Recovery Time Objective (RTO) of four hours and a Recovery Point Objective (RPO) of one hour or less. Additionally, he requests that you implement the solution within two weeks.
Your database is 200GB in size, and your Internet connection is 20Mbps.

How would you do this while keeping prices low?

- 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.

Commented [LC414]: This is what it's called Pilot Light approach with only DB running and replicate while you have preconfigured AMI and autoscaling config

In a Pilot Light Disaster Recovery scenario option, a minimal version of an environment is always running in the cloud, which basically host the critical functionalities of the application for e.g., databases

While VPN can be setup quickly asynchronous replication using VPN would work, running instances in DR is expensive)

EC2 running in Compute Optimized as well as Direct Connect is expensive to start with also Direct Connect cannot be implemented in 2 weeks

while AMI is a right approach to keep cost down, Upload to S3 very Slow

Question #731

A business requires that only particularly hardened AMIs be launched into public subnets inside a VPC, and that the AMIs be associated with a certain security group. Allowing non-compliant instances to launch onto the public subnet may provide a severe security risk if permitted to run. A mapping of permitted AMIs to subnets and security groups occurs in the same AWS account's Amazon DynamoDB database. The business developed an AWS Lambda function that, when run, terminates an Amazon EC2 instance if the AMI, subnet, and security group combination is not authorized in the DynamoDB database.

What should the Solutions Architect do to limit the risk of compliance deviations as fast as possible?

- 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.

Commented [LC415]: D after reading this document https://d1.awsstatic.com/whitepapers/aws-building-ami-factory-process-using-ec2-ssm-marketplace-and-service-catalog.pdf

A: This covers the harden AMI but not non-compliant ones. We want to execute the termination when the non-compliant instances are launched, not the opposite.

B: S3 event notification has no filter.

C: Too tedious

Question #732

You have purchased a support plan for AWS Business and Enterprise.
Your organization is experiencing a backlog of issues, and around 20 of your IAM users are required to initiate technical support cases.

How many users are permitted to open technical support tickets under the AWS Business and Enterprise support plans?

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

Commented [LC416]: https://aws.amazon.com/premiumsupport/faqs/

Q: How many users can open technical support cases?

The Business and Enterprise Support plans allow an unlimited number of users to open technical support cases (supported by AWS Identity and Access Management (IAM)). The Developer Support plan allows one user to open technical support cases. Customers with the Basic Support plan cannot open technical support cases.
C is correct

Question #733

A retail firm processes point-of-sale data in its data center using application servers and publishes the results to an Amazon DynamoDB database. The data center is linked to the company's VPC through an AWS Direct Connect (DX) connection, and the application servers need a reliable network connection with a minimum of 2 Gbps.
The organization determines that the DynamoDB table should be highly available and fault tolerant. According to corporate policy, data should be accessible in two areas.

What modifications should the business make to comply with these requirements?

- A. Establish a second DX connection for redundancy. Use DynamoDB global tables to replicate data to a second Region. Modify the application to fail over to the second Region.
- B. Use an AWS managed VPN as a backup to DX. Create an identical DynamoDB table in a second Region. Modify the application to replicate data to both Regions.
- C. Establish a second DX connection for redundancy. Create an identical DynamoDB table in a second Region. Enable DynamoDB auto scaling to manage throughput capacity. Modify the application to write to the second Region.
- D. Use AWS managed VPN as a backup to DX. Create an identical DynamoDB table in a second Region. Enable DynamoDB streams to capture changes to the table. Use AWS Lambda to replicate changes to the second Region.

Commented [LC417]: VPN doesn't meet the bandwidth. The maximum bandwidth of VPN is 1.25Gbps.

https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-limits.html

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html

Question #734

A corporation is preparing to introduce a new billing application in two weeks. The application is being tested on ten Amazon EC2 instances controlled by an Auto Scaling group in the subnet 172.31.0.0/24 of VPC A with the CIDR block 172.31.0.0/16. The developers saw connection timeout issues in the application logs while attempting to connect to an Oracle database operating on an Amazon EC2 instance in the same region under VPC B with CIDR block 172.50.0.0/16.
The database instance's IP address is hard-coded into the application instances.

Which suggestions should a Solutions Architect provide to the Developers in order to resolve the issue in the most secure manner possible with the least amount of maintenance and overhead?

- A. Disable the SrcDestCheck attribute for all instances running the application and Oracle Database. Change the default route of VPC A to point ENI of the Oracle Database that has an IP address assigned within the range of 172.50.0.0/16
- B. Create and attach internet gateways for both VPCs. Configure default routes to the internet gateways for both VPCs. Assign an Elastic IP for each Amazon EC2 instance in VPC A
- C. Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 172.50.0.0/16
- D. Create an additional Amazon EC2 instance for each VPC as a customer gateway; create one virtual private gateway (VGW) for each VPC, configure an end- to-end VPC, and advertise the routes for 172.50.0.0/16

Commented [LC418]: C
A: It does not go through NAT so this is not the solution.
B: It does not need to go through internet. This is not secured.
D: This is VPN which is not suitable. Peering should be used.

Question #735

A business has an application that sells tickets online and sees spikes in demand every seven days. The program is comprised of a stateless display layer that runs on Amazon EC2, an Oracle database for storing unstructured data catalog information, and a backend API layer. The front-end layer distributes the load over nine On-Demand instances spread across three Availability Zones through an Elastic Load Balancer (AZs). Oracle is being run on a single EC2 instance. When conducting more than two continuous campaigns, the firm has performance challenges. A solutions architect is responsible for developing a solution that satisfies the following requirements:

⇨ Address scalability issues.
⇨ Increase the level of concurrency.
⇨ Eliminate licensing costs.
⇨ Improve reliability.

Which procedure should the solutions architect follow?

- A. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the Oracle database into a single Amazon RDS reserved DB instance.
- B. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Create two additional copies of the database instance, then distribute the databases in separate AZs.
- C. Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs. Convert the tables in the Oracle database into Amazon DynamoDB tables.
- D. Convert the On-Demand Instances into Spot instances to reduce costs for the front end. Convert the tables in the Oracle database into Amazon DynamoDB tables.

Commented [LC419]: C is the right answer.

A: single RDS doesn't improve reliability
B: two additional copies of the Oracle database doesn't eliminate licensing costs
D: doesn't address the scalability issues

To avoid licensing you can't use Oracle on RDS or EC2.

Question #736

When utilizing string conditions inside IAM, it is possible to utilize condensed versions of the available comparators rather than the more verbose ones.

streqi is the abbreviation for the _____ string condition.

- A. StringEqualsIgnoreCase
- B. StringNotEqualsIgnoreCase
- C. StringLikeStringEquals
- D. StringNotEquals

Commented [LC420]: When using string conditions within IAM, short versions of the available comparators can be used instead of the more verbose versions. For instance, streqi is the short version of StringEqualsIgnoreCase that checks for the exact match between two strings ignoring their case.
Reference:
http://awsdocs.s3.amazonaws.com/SNS/20100331/sns-gsg-2010-03-31.pdf

Question #737

A business that specializes in the Internet of Things has deployed a fleet of sensors to monitor temperatures in distant regions. Each device establishes a connection with AWS IoT Core and transmits a message every 30 seconds, which updates an Amazon DynamoDB database. A system administrator uses AWS IoT to check that devices are still communicating with AWS IoT Core: the database is not updating.

What should a Solutions Architect look for when a database is not being updated?

- A. Verify the AWS IoT Device Shadow service is subscribed to the appropriate topic and is executing the AWS Lambda function.
- B. Verify that AWS IoT monitoring shows that the appropriate AWS IoT rules are being executed, and that the AWS IoT rules are enabled with the correct rule actions.
- C. Check the AWS IoT Fleet indexing service and verify that the thing group has the appropriate IAM role to update DynamoDB.
- D. Verify that AWS IoT things are using MQTT instead of MQTT over WebSocket, then check that the provisioning has the appropriate policy attached.

Commented [LC421]: B - choose the appropriate actions on the rule. in this case write to DDB.
https://docs.aws.amazon.com/iot/latest/developerguide/iot-rule-actions.html

https://docs.aws.amazon.com/iot/latest/developerguide/dynamodb-rule-action.html

Question #738

A user considers using the EBS PIOPS volume.

Which of the following alternatives is the most appropriate use case for the PIOPS EBS volume?

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

Commented [LC422]: C.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html
"...Provisioned IOPS SSD (io1 and io2) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency..."

Question #739 (EXAM)

A solutions architect is developing a web application that will be hosted on an Amazon RDS for PostgreSQL database. The database instance is projected to get a much greater number of reads than writes. The architect of the solution must guarantee that the high volume of read traffic can be handled and that the database instance is highly available.

What procedures should the solutions architect take to ensure compliance with these requirements? (Select three.)

- A. Create multiple read replicas and put them into an Auto Scaling group.
- B. Create multiple read replicas in different Availability Zones.
- C. Create an Amazon Route 53 hosted zone and a record set for each read replica with a TTL and a weighted routing policy.
- D. Create an Application Load Balancer (ALB) and put the read replicas behind the ALB.
- E. Configure an Amazon CloudWatch alarm to detect a failed read replica. Set the alarm to directly invoke an AWS Lambda function to delete its Route 53 record set.
- F. Configure an Amazon Route 53 health check for each read replica using its endpoint.

Commented [LC423]: It's B C F
You can use Amazon Route 53 weighted record sets to distribute requests across your read replicas. Within a Route 53 hosted zone, create individual record sets for each DNS endpoint associated with your read replicas and give them the same weight. Then, direct requests to the endpoint of the record set.
You can incorporate Route 53 health checks to be sure that Route 53 directs traffic away from unavailable read replicas

Commented [LC424]:

Commented [LC425]:

Question #740

In terms of the AWS Lambda permissions paradigm, when you construct a Lambda function, you define an IAM role that AWS Lambda may take in order to run the Lambda function on your behalf. Additionally, this job is referred to as the _____ role.

- A. configuration
- B. execution
- C. delegation
- D. dependency

Commented [LC426]: 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.
Reference:
http://docs.aws.amazon.com/lambda/latest/dg/lambda-dg.pdf

Question #741

Your organization previously created a highly trafficked, dynamically routed VPN connection between your on-premises data center and AWS. You recently provisioned a DirectConnect connection and want to begin utilizing it.

Which of the following alternatives, after establishing DirectConnect settings in the AWS Console, will offer the smoothest 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 man your VPN router, verify network traffic is leveraging Directconnect and then delete your existing VPN connection.
- C. Update your VPC route tables to point to the DirectConnect connection configure your DirectConnect router with the appropriate settings verify network traffic is leveraging DirectConnect and then delete the VPN connection.
- D. Configure your DirectConnect router, update your VPC route tables to point to the DirectConnect connection, configure your VPN connection with a higher BGP priority, and verify network traffic is leveraging the DirectConnect connection.

Commented [LC427]: Answer is B
We can have only 1 VGW on VPC, so no need to configure route in VPC anymore
https://acloud.guru/forums/aws-certified-solutions-architect-professional/discussion/-KWVDow4aXPEdVfmBcZD/after-configuring-directconnect-settings-in-the-aws-console-which-of-the-followi

https://aws.amazon.com/blogs/networking-and-content-delivery/creating-active-passive-bgp-connections-over-aws-direct-connect/

Question #742

What is the network performance of the Amazon EC2 c4.8xlarge instance?

- A. Very High but variable
- B. 20 Gigabit
- C. 5 Gigabit
- D. 10 Gigabit

Commented [LC428]: Networking performance offered by the c4.8xlarge instance is 10 Gigabit.
Reference:
http://aws.amazon.com/ec2/instance-types/

Question #743

A corporation uses AWS to host a three-tier application. According to users, application speed varies significantly depending on the time of day and feature engaged.
Components of the application include the following:
⇨ 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.
The web and application layers have been identified as network limited by operations.

Which of the following methods is the most cost effective for increasing application performance? (Select 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

Commented [LC429]: B: use autoscaling, and that allow for increasing and reducing of utilization, plus the performance of M4 is better.
D: using CloudFront, reduce the network local utilization, thus support the solution.

Commented [LC430]:

Question #744

You intend to utilize Amazon Redshift and will be deploying dw1.8xlarge nodes.

What is the bare minimum number of nodes that you must deploy in this configuration?

- A. 1
- B. 4
- C. 3
- D. 2

Commented [LC431]: 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.
Reference:
http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-clusters.html

Question #745

A business is in the process of transferring its apps to AWS. The apps will be deployed to business units' AWS accounts. The firm employs many development teams that are responsible for the creation and maintenance of all apps. The firm anticipates tremendous user growth.
The chief technology officer of the organization must have the following requirements:
⇨ Developers must launch the AWS infrastructure using AWS CloudFormation.
⇨ Developers must not be able to create resources outside of CloudFormation.
⇨ The solution must be able to scale to hundreds of AWS accounts.

Which of the following would satisfy these criteria? (Select two.)

- A. Using CloudFormation, create an IAM role that can be assumed by CloudFormation that has permissions to create all the resources the company needs. Use CloudFormation StackSets to deploy this template to each AWS account.
- B. In a central account, create an IAM role that can be assumed by developers, and attach a policy that allows interaction with CloudFormation. Modify the AssumeRolePolicyDocument action to allow the IAM role to be passed to CloudFormation.
- C. Using CloudFormation, create an IAM role that can be assumed by developers, and attach policies that allow interaction with and passing a role to CloudFormation. Attach an inline policy to deny access to all other AWS services. Use CloudFormation StackSets to deploy this template to each AWS account.
- D. Using CloudFormation, create an IAM role for each developer, and attach policies that allow interaction with CloudFormation. Use CloudFormation StackSets to deploy this template to each AWS account.
- E. In a central AWS account, create an IAM role that can be assumed by CloudFormation that has permissions to create the resources the company requires. Create a CloudFormation stack policy that allows the IAM role to manage resources. Use CloudFormation StackSets to deploy the CloudFormation stack policy to each AWS account.

Commented [LC432]: A over E because stack policies are used only for updates and as well to avoid any unintentional updates. In this scenario, they had not discussed the requirement of updates on the resources of CloudFormation stack. You need to deploy the CF template and not just the stack policy.

Commented [LC433]:

Question #746

If no explicit deny is discovered when IAM's Policy Evaluation Logic is applied, the enforcement code searches for any _____ commands that apply to the request.

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

Commented [LC434]: 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.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

Question #747

A large firm is developing a platform for infrastructure services for its consumers. The following conditions have been established by the company:
⇨ Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services.
⇨ Use a central account to manage the creation of infrastructure services.
⇨ Distribute infrastructure services across many AWS Organizations accounts.
⇨ Allow for the enforcement of tags on any infrastructure that is initiated by users.

Which combination of AWS services-based activities will satisfy these requirements? (Select three.)

- A. Develop infrastructure services using AWS Cloud Formation templates. Add the templates to a central Amazon S3 bucket and add the-IAM roles or users that require access to the S3 bucket policy.
- B. Develop infrastructure services using AWS Cloud Formation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.
- C. Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.
- D. Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption assign users access and apply launch constraints.
- E. Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company. Apply the TagOption to AWS Service Catalog products or portfolios.
- F. Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

Commented [LC435]: https://docs.aws.amazon.com/servicecatalog/latest/adminguide/tagoptions.html

Commented [LC436]:

Commented [LC437]:

Question #748

How much memory is provided by the cr1.8xlarge instance type?

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

Commented [LC438]: Worthless question.

https://www.ec2instances.info/?selected=cr1.8xlarge

Question #749

A company runs an e-commerce platform with front-end and e-commerce tiers. Both tiers run on LAMP stacks with the front-end instances running behind a load balancing appliance that has a virtual offering on AWS. Currently, the Operations team uses SSH to log in to the instances to maintain patches and address other concerns. The platform has recently been the target of multiple attacks, including

⇨ A DDoS attack.
⇨ An SQL injection attack.
⇨ Several successful dictionary attacks on SSH accounts on the web servers.

The company wants to improve the security of the e-commerce platform by migrating to AWS. The company's Solutions Architects have decided to use the following approach:

⇨ Code review the existing application and fix any SQL injection issues.
⇨ Migrate the web application to AWS and leverage the latest AWS Linux AMI to address initial security patching.
⇨ Install AWS Systems Manager to manage patching and allow the system administrators to run commands on all instances, as needed.

What further efforts will address the threat types identified while maintaining high availability and lowering risk?

- A. Enable SSH access to the Amazon EC2 instances using a security group that limits access to specific IPs. Migrate on-premises MySQL to Amazon RDS Multi-AZ. Install the third-party load balancer from the AWS Marketplace and migrate the existing rules to the load balancer's AWS instances. Enable AWS Shield Standard for DDoS protection.
- B. Disable SSH access to the Amazon EC2 instances. Migrate on-premises MySQL to Amazon RDS Multi-AZ. Leverage an Elastic Load Balancer to spread the load and enable AWS Shield Advanced for protection. Add an Amazon CloudFront distribution in front of the website. Enable AWS WAF on the distribution to manage the rules.
- C. Enable SSH access to the Amazon EC2 instances through a bastion host secured by limiting access to specific IP addresses. Migrate on-premises MySQL to a self-managed EC2 instance. Leverage an AWS Elastic Load Balancer to spread the load and enable AWS Shield Standard for DDoS protection. Add an Amazon CloudFront distribution in front of the website.
- D. Disable SSH access to the EC2 instances. Migrate on-premises MySQL to Amazon RDS Single-AZ. Leverage an AWS Elastic Load Balancer to spread the load. Add an Amazon CloudFront distribution in front of the website. Enable AWS WAF on the distribution to manage the rules.

Commented [LC439]: B
A: Does not need third party load balancer.
C: SSH should be disabled and commands run from System Manager. SQL needs to be more highly available and not on a single EC2 instance.
D: DB should be multi-AZ. DDOS protection needs Shield.

Question #750

Amazon Cognito authenticates your mobile app with the Identity Provider (IdP) using the provider's SDK. After authenticating the end user with the IdP, your app passes the OAuth or OpenID Connect token given by the IdP to Amazon Cognito, which provides 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

Commented [LC440]: 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.
Reference:
http://aws.amazon.com/cognito/faqs/

Question #751

A business wishes to relocate its on-premises data center to the Amazon Web Services (AWS) Cloud. This comprises hundreds of virtualized Linux and Microsoft Windows servers, storage area networks (SANs), Java and PHP applications running on MYSQL and Oracle databases. Numerous departmental services are hosted either in-house or elsewhere.
Technical documentation is insufficient and out of current. A solutions architect must comprehend the present environment and forecast the cost of cloud resources after the move.

Which tools or services should a solutions architect use while planning a cloud migration? (Choose three.)

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS X-Ray
- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

Commented [LC441]: ADF
- Use AWS Application Discovery Service to gather information about the running virtual machines and running applications inside the servers.

- Use the AWS Cloud Adoption Readiness Tool (CART) to generate a migration assessment report to identify gaps in organizational skills and processes.

- Use AWS Migration Hub to discover and track the status of the application migration across AWS and partner solutions.

Question #752

Which security components of AWS are the customer's responsibility? (Select 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

Commented [LC442]:

Commented [LC443]:

Commented [LC444]:

Commented [LC445]:

Commented [LC446]:

Commented [LC447]:

Question #753

A business operates a well-known public-facing ecommerce website. Its user base is rapidly expanding from a local to a national level. The website is hosted in-house using web servers and a MySQL database. The business wishes to move its burden to AWS. A solutions architect must develop a solution for the following:
⇨ Improve security
⇨ Improve reliability
⇨ Improve availability
⇨ Reduce latency
⇨ Reduce maintenance

Which measures should the solutions architect do in combination to satisfy these requirements? (Select three.)

- A. Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer.
- B. Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster.
- C. Use Amazon EC2 instances in two Availability Zones to host a highly available MySQL database cluster.
- D. Host static website content in Amazon S3. Use S3 Transfer Acceleration to reduce latency while serving webpages. Use AWS WAF to improve website security.
- E. Host static website content in Amazon S3. Use Amazon CloudFront to reduce latency while serving webpages. Use AWS WAF to improve website security.
- F. Migrate the database to a single-AZ Amazon RDS for MySQL DB instance.

Commented [LC448]:

Commented [LC449]:

Commented [LC450]:

Question #754

A read-only news reporting site with a mixed web and application layer and a database tier that faces high and unexpected traffic demands must be able to adapt automatically to these changes.

Which Amazon Web Offerings (AWS) services should be employed to achieve 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.

Commented [LC451]:

Question #755

A business intends to restructure a monolithic application into a contemporary application architecture that will be delivered on Amazon Web Services. The CI/CD pipeline must be improved to accommodate the application's contemporary architecture, which includes the following requirements:
⇨ It should allow changes to be released several times every hour.
⇨ It should be able to roll back the changes as quickly as possible.

Which design will satisfy these criteria?

- A. Deploy a CI/CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances.
- B. Specify AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application. To deploy, swap the staging and production environment URLs.
- C. Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment.
- D. Roll out the application updates as part of an Auto Scaling event using prebuilt AMIs. Use new versions of the AMIs to add instances, and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

Commented [LC452]: B is the right answer. It is the fastest when it comes to rollback and deploying changes every hour. C is good but it falls short to meet the requirement of frequent deployments as it is pretty heavy in terms of having to build a new infrastructure each time a new deployment is needed.

Question #756

Your system was recently unavailable due to the troubleshooting procedure. You discovered that a new administrator killed multiple production EC2 instances by mistake.

Which of the following techniques will assist in preventing a repeat of this incident in the future?

The administrator must continue to have the ability 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.

Commented [LC453]: B is the right answer.

D can't discriminate DEV and PROD.

Question #757

When you load your table straight from an Amazon _____ table, you have the option of limiting the amount of provided throughput used.

- A. RDS
- B. DataPipeline
- C. DynamoDB
- D. S3

Commented [LC454]: 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.

Reference:
http://docs.aws.amazon.com/redshift/latest/dg/t_Loading_tables_with_the_COPY_command.html

Question #758

Temporary security credentials for an IAM user are normally good for 12 hours, but you may request a length of up to __ hours.

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

Commented [LC455]: 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.
Reference:
http://docs.aws.amazon.com/STS/latest/UsingSTS/CreatingSessionTokens.html

Question #759

You've created a VPC with a CIDR block of 10.0.0.0/28 and deployed a three-tier web application. Two web servers, two application servers, two database servers, and one NAT instance are originally deployed to a total of seven EC2 instances. Two availability zones are used to distribute the web, application, and database servers (AZs). Additionally, you deploy an ELB in front of the two web servers and use Route53 for DNS Web (raffle gradually increases in the days following the deployment, and you attempt to double the number of instances in each tier of the application to handle the increased load; however, some of these new instances fail to launch.

Which of the following is the most likely cause? (Select two.)

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

Commented [LC456]: C, E are correct indeed.

10.0.0.0/28 has 14 ips available. Precisely,
from 10.0.0.1
to 10.0.0.14

4 ips are reserved so availables ips are from 10.0.0.1 to 10.0.0.10

known fixed ips by reqs are 7 ips
variable ips are dictated by the Balancers, at least 1.
so at least 8 ips are busy, making only 2 ips for scaling up.

Hence, C, E.

Commented [LC457]:

Question #760

Dave is Example Corp.'s primary administrator, and he chooses to employ paths to better segment the company's users, creating a distinct administrator group for each path-based division. The following is a partial list of the routes he intends to take:

/marketing
/sales
/legal

Dave establishes a new administrator group called Marketing Admin for the company's marketing department.
He categorizes it as /marketing. arn:aws:iam::123456789012:group/marketing/Marketing_Admin is the group's ARN.

Dave creates the Marketing Admin group and grants it authority to perform all IAM activities on all groups and users on the /marketing route. Additionally, the policy grants the Marketing Admin group authority to conduct any AWS S3 activities on the items in the corporate bucket's section.

```
{
"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

Commented [LC458]: Very weird question and badly written. Should be B because it says that the Marketing Admin should be able to IAM admin under route /marketing. But the policy explicitely denies that.

Question #761

A big multinational corporation wishes to deploy a stateless mission-critical application to Amazon Web Services (AWS). On a z/OS operating system, the application is built on IBM WebSphere (application and integration middleware), IBM MQ (messaging middleware), and IBM DB2 (database software).

What procedures should the Solutions Architect follow while migrating 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.

Commented [LC459]: B
A\C: RDS only Supports Aurora, PostgreSQL, MySQL, MariaDB, Oracle & MS SQL Server.
D: SMS cannot migrate from a z/OS, it can only migrate from VMware or HyperV. It basically replaces VM Import.
https://aws.amazon.com/blogs/database/aws-database-migration-service-and-aws-schema-conversion-tool-now-support-ibm-db2-as-a-source/
https://aws.amazon.com/quickstart/architecture/ibm-mq/

Question #762

You've been suggested a new customer, and you know he's into online gaming. You're pretty confident he'll want to build up an online gaming site, which will need a database service that delivers quick and reliable performance with seamless scalability.

Which of the following Amazon Web Services databases is the greatest fit for an online gaming website?

- A. Amazon SimpleDB
- B. Amazon DynamoDB
- C. Amazon Redshift
- D. Amazon ElastiCache

Commented [LC460]: ElastiCache is a cache service. Redshift is a Data Warehouse service.

SimpleDB may be used for the gaming service itself like saving the session state or showing leaderboards. But, for the website, Dynamo is the best.

Question #763

Amazon S3 is used by a business to store documents that are exclusively accessible through an Amazon EC2 instance in a particular virtual private cloud (VPC). The organization is concerned that a hostile insider with access to this instance may also create an EC2 instance in another VPC and use it to access these data.

Which of the following options provide the needed level of protection?

- A. Use an S3 VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint.
- B. Use EC2 instance profiles and an S3 bucket policy to limit access to the role attached to the instance profile.
- C. Use S3 client-side encryption and store the key in the instance metadata.
- D. Use S3 server-side encryption and protect the key with an encryption context.

Commented [LC461]: Answer is A, Endpoint connections cannot be extended out of a VPC.

Question #764 (SKIP)

How can a user access the IAM Role that was established as part of the launch configuration?

- 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

Commented [LC462]: It is now IamInstanceProfile option

https://docs.aws.amazon.com/cli/latest/reference/autoscaling/describe-launch-configurations.html

A is the closest to be the correct one. This question is probably to be old.

Question #765

You establish a virtual private network (VPN) connection, and your VPN device supports the Border Gateway Protocol (BGP).

Which of the following should be mentioned during the VPN connection's configuration?

- A. Classless routing
- B. Classfull routing
- C. Dynamic routing
- D. Static routing

Commented [LC463]:

Question #766

A business has many teams, and each team has its own Amazon RDS database with a total capacity of 100 TB. The firm is developing a data query platform that will enable Business Intelligence Analysts to create a weekly business report. The new system must be capable of doing ad-hoc SQL queries.

Which approach is the MOST cost-effective?

- 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.

Commented [LC464]: Athena is the cheapest option to run query. D is the answer.

Question #767

A Solutions Architect is responsible for designing a highly available application that enables authorized users to remain connected to the application even when underlying components fail.

Which solution will satisfy these criteria?

- 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.

Commented [LC465]:

Question #768

In Amazon ElastiCache, the loss of a single cache node might affect the availability of your application and the strain on your back-end database, while ElastiCache creates a new cache node and populates it.

Which of the following is a solution for mitigating this possible effect on availability?

- 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.

Commented [LC466]: 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.

Reference:
http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/CacheNode.Memcached.html

Question #769

You're going to use AWS Direct Connect. You want to access AWS public service endpoints such as Amazon S3 using the AWS Direct Connect connection. You want other Internet traffic to utilize your current Internet Service Provider connection.

How should AWS Direct connect be configured 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.

Commented [LC467]: C is correct as we need to use public VIF on direct link to connect to S3. BGP protocol is used for dynamic, hence option A is eliminated.

Ref. https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-access-direct-connect/

Question #770

A user is attempting to comprehend the intricacies of the CloudWatch monitoring concept.

Which of the following services does not provide comprehensive monitoring through CloudWatch?

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

Commented [LC468]: Debugging with EMR is a messy task!

Question #771

If you have a running instance that is utilizing an Amazon EBS boot partition, you may use the _____ API to free up compute resources while maintaining the boot partition's data.

- A. Stop Instances
- B. Terminate Instances
- C. AMI Instance
- D. Ping Instance

Commented [LC469]: 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.

Reference:
https://aws.amazon.com/ec2/faqs/#How_quickly_will_systems_be_running

Question #772

You've created a CloudFormation template that deploys a single Elastic Load Balancer in front of two EC2 Instances.

Which portion of the template should you alter to ensure that the load balancer's DNS is returned when the stack is created?

- A. Parameters
- B. Outputs
- C. Mappings
- D. Resources

Commented [LC470]: In the following example, the output named BackupLoadBalancerDNSName returns the DNS name for the resource with the logical ID BackupLoadBalancer only when the CreateProdResources condition is true. (The second output shows how to specify multiple outputs.)

"Outputs" : {
"BackupLoadBalancerDNSName" : {
"Description": "The DNSName of the backup load balancer",
"Value" : { "Fn::GetAtt" : ["BackupLoadBalancer",
"DNSName"]}, "Condition" :
"CreateProdResources"
},
"InstanceID" : {
"Description": "The Instance ID", "Value" : { "Ref" :
"EC2Instance" }
}}

Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html

Question #773

You wish to use DNS names to mount an Amazon EFS file system on an Amazon EC2 instance.

Which of the following generic DNS names for a mount target must you use when mounting the file system?

- A. availability-zone.file-system-id.efs.aws-region.amazonaws.com
- B. efs-system-id.availability-zone.file-aws-region.amazonaws.com
- C. $file-system-id.$availability-zone.$efs.aws-region.$amazonaws.com
- D. #aws-region.#availability-zone.#file-system-id.#efs.#amazonaws.com

Commented [LC471]: Answer is A here

https://docs.aws.amazon.com/efs/latest/ug/mounting-fs-mount-cmd-dns-name.html

Mount target DNS name – In December 2016, we introduced file system DNS names. We continue to provide a DNS name for each Availability Zone mount target for backward compatibility. The generic form of a mount target DNS name is as follows.

availability-zone.file-system-id.efs.aws-region.amazonaws.com

Question #774

Which of the following IAM policy components allows for the definition of an exception to a set of actions?

- A. NotException
- B. ExceptionAction
- C. Exception
- D. NotAction

Commented [LC472]:

Question #775

A Solutions Architect is tasked with the responsibility of developing a cost-effective backup solution for a company's 500MB source code repository, which contains proprietary and sensitive applications. The repository is Linux-based and does daily tape backups. Backup tapes are retained for one year.
The existing solution does not satisfy the demands of the firm since it is a manual process that is prone to mistake, costly to maintain, and does not fulfill the need for a Recovery Point Objective (RPO) of 1 hour or a Recovery Time Objective (RTO) of 2 hours. The new disaster recovery criteria are that backups be kept offshore and that a single file may be restored if necessary.

Which solution satisfies the customer's RTO, RPO, and disaster recovery requirements with the LEAST amount of work 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 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.

Commented [LC473]: Tough question. I do support answer "B".
Even though there is no cross-region replication, but that is not a requirement in the question. The requirement is just an offsite (AWS) disaster recovery. Therefore, a single copy in AWS would make the deal.
Also, there is a tricky requirement of restoring a SINGLE FILE! The snapshot of Storage Gateway (cached or stored, or tape) are storing the backup as a whole, and not as files! that mean to restore, you need to build a snapshot, and mount the snapshot into an EC2, then restore the files. Therefore, it needs effort to restore, un-like the (File storage), which store the files as they are in S3 bucket! Where pulling a file is very straight forward.

https://d1.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf

A: nightly backup, does not meet the requirement. Plus, restoration effort.

C & D: both are working solutions, and valid too. However, restoration effort, and cost is higher than B.

Again, it is a tough decision.

Question #776

According to a security engineer, an existing program receives credentials for an Amazon RDS for MySQL database from an encrypted file stored in Amazon S3. The security engineer want to enhance the application's security in the next version by implementing the following improvements to the application's design:

⇨ The database must use strong, randomly generated passwords stored in a secure AWS managed service.
⇨ The application resources must be deployed through AWS CloudFormation.
⇨ The application must rotate credentials for the database every 90 days.

To deploy the application, a solutions architect will create a CloudFormation template.

Which CloudFormation resources will match the criteria of the security engineer with the LEAST amount of operational overhead?

- A. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
- B. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- C. Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

Commented [LC474]: C is A with extra steps. D, B are wrong.

https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_customize.html

Question #777 (SKIP)

Which RAID configuration is utilized on the Cloud Block Storage back-end to provide the highest possible degree 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)

Commented [LC475]: Is this AWS related? I guess C would be the answer.

Question #778

On AWS, a huge multinational corporation hosts a timesheet application that is utilized by employees worldwide. The application is hosted on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer and uses an Amazon RDS MySQL Multi-AZ database instance for data storage.

The CFO is worried about the business's potential effect if the application is unavailable. The application's downtime cannot exceed two hours, and the solution must be as cost-effective as feasible.

How should the Solutions Architect balance the needs of the CFO with the goal of reducing 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.

Commented [LC476]: Both C and D look like good options. C should be better in terms of being "cost-effective".

The RTO is 2 hours, which has nothing to do with the RPO which is NOT SPECIFIED.

Answer "C" builds in a one-hour outage every day and effectively creates a 24hr RPO. Cross-region replication provides data durability and is in alignment with best practices but has NOTHING TO DO with the CIO requirements in the question.

The requirement is: "A cost effective way to ensure no more than 2 hours of application downtime."

Running a read replica doesn't grant MORE uptime than a snapshot (it does improve performance) if you have to rebuild the application from a CF template in a new region anyway.

Anyone choosing "D" either didn't read the question closely or doesn't understand very well the difference between a read replica and a snapshot.

Question #779

Which characteristic of the load balancing service aims to send future connections to a service to the same node as long as it is online?

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

Commented [LC477]: Is this a wrong question? In AWS that's called 'sticky session'

Question #780

What is the maximum length of an AWS IAM instance profile name?

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

Commented [LC478]: http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.html

Question #781

Which of the striping options available for EBS volumes has the drawback of 'Doubling the amount of I/O needed from the instance to EBS in comparison to RAID 0, since you're mirroring all writes to a pair of volumes, limiting the amount of striping possible.'?

- A. Raid 1
- B. Raid 0
- C. RAID 1+0 (RAID 10)
- D. Raid 2

Commented [LC479]: Raid 1 is referred as 'mirroring' and it's the right answer.

Ref.
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html

Question #782

CloudWatch receives a custom metric from a user.

If several calls to the CloudWatch APIs have different dimensions but the same metric name, how would CloudWatch handle them all?

- A. It will reject the request as there cannot be a separate dimension for a single metric.
- B. It will group all the calls into a single call.
- C. It will treat each unique combination of dimensions as a separate metric.
- D. It will overwrite the previous dimension data with the new dimension data.

Commented [LC480]: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-rotate-certificates.html

Question #783

You're attempting to remove an SSL certificate from the IAM certificate store and get the following message: "Certificate: <certificate-id> is currently in use by CloudFront."

Which of the following assertions is most likely the cause of 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.

Commented [LC481]: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-rotate-certificates.html

Question #784

A multimedia firm is creating an application for a worldwide user base using a single AWS account. The storage and bandwidth need of an application are unexpected. As the web layer, the application will employ Amazon EC2 instances behind an Application Load Balancer, while the database tier will use Amazon DynamoDB. The application's environment must match the following requirements:

⇨ Low latency when accessed from any part of the world
⇨ WebSocket support
⇨ End-to-end encryption
⇨ Protection against the latest security threats
⇨ Managed layer 7 DDoS protection

What activities should the solutions architect take to ensure compliance with these requirements? (Select two.)

- A. Use Amazon Route 53 and Amazon CloudFront for content distribution. Use Amazon S3 to store static content
- B. Use Amazon Route 53 and AWS Transit Gateway for content distribution. Use an Amazon Elastic Block Store (Amazon EBS) volume to store static content
- C. Use AWS WAF with AWS Shield Advanced to protect the application
- D. Use AWS WAF and Amazon Detective to protect the application
- E. Use AWS Shield Standard to protect the application

Commented [LC482]:

Commented [LC483]: AWS Shield Advanced is necessary for L7 protection

Question #785

A business has an internal AWS Elastic Beanstalk worker environment contained inside a VPC that requires access to an external payment gateway API accessible through an HTTPS endpoint on the public internet. Due to security restrictions, the application team at the payment gateway may allow access to just one public IP address.

Which architecture will configure an Elastic Beanstalk environment for accessing the firm's application without requiring the company to make many changes?

- 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.

Commented [LC484]: A is the right answer.

Ref:
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/vpc.html

Question #786

To handle Web traffic for a popular product, your chief financial officer and information technology director have purchased ten m1.large high-utilization Reserved Instances (RIs) that are evenly distributed across two availability zones; Route 53 is used to route the traffic to an Elastic Load Balancer (ELB). After a few months, the product becomes even more popular, necessitating the augmentation of capacity. As a consequence, your organization acquires two C3.2xlarge Ris with a medium usage rate. You register the two c3.2xlarge instances with your ELB and shortly discover that the m1.large instances are fully used but the c3.2xlarge instances have substantial unused capacity.

Which option is the most cost effective and makes the most use of EC2 capacity?

- 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.

Commented [LC485]: D must be the answer.

A, B if you have already purchase Reversed Instance (RIs) so if you shutdown either of them, you still lose the cost.

C. It does not work well, as Route53 can't route to EC2 unless it has EIP because its IP will change when rebooted. You will need EIPs for all EC2s. So it is impossible solution. R53 doesnt work that way, it is not a intra-regional load balancer. The closest it can get to inter regional load balancing is a multi-value response and then letting the client decide which IP to use

D make sense, the traffic for each instance was loaded-balance however the improper type between C2 and M1 cause the CPU on M1 meanwhile no load on C2. You need another ELB, one for C2 group and one for M1 group; then route the traffic 80% to C1 and 20% to C1 for example.

Question #787

What happens when a VPC's dedicated instances are launched?

- A. If you launch an instance into a VPC that has an instance tenancy of dedicated, you must manually create a Dedicated instance.
- B. If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is created as a Dedicated instance, only based on the tenancy of the instance.
- C. If you launch an instance into a VPC that has an instance tenancy of dedicated, your instance is automatically a Dedicated instance, regardless of the tenancy of the instance.
- D. None of these are true.

Commented [LC486]: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-usage-overview.html#creatingdedicatedvpc

Question #788

Which of the following is not included in the billing metrics delivered to Amazon CloudWatch by Billing?

- 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

Commented [LC487]: https://aws.amazon.com/fr/blogs/aws/monitor-estimated-costs-using-amazon-cloudwatch-billing-metrics-and-alarms/

Question #789

Is it possible to have a direct connection to Amazon Web Services (AWS)?

- A. No, AWS only allows access from the public Internet.
- B. No, you can create an encrypted tunnel to VPC, but you cannot own the connection.
- C. Yes, you can via Amazon Dedicated Connection
- D. Yes, you can via AWS Direct Connect.

Commented [LC488]:

Question #790

Identify an application that monitors AWS Data Pipeline for new jobs and then executes them.

- A. A task executor
- B. A task deployer
- C. A task runner
- D. A task optimizer

Commented [LC489]: https://docs.aws.amazon.com/datapipeline/latest/DeveloperGuide/dp-how-remote-taskrunner-client.html

Question #791

The data science team at a large corporation wants to create a secure, cost-effective method for providing quick access to Amazon SageMaker. The data scientists are unfamiliar with AWS and want the ability to deploy a Jupyter notebook instance. The notebook instance must be prepared with an AWS KMS key in order to encrypt data at rest on the machine learning storage volume without disclosing the extensive setup requirements.

Which strategy enables the business to provide a self-service mechanism for data scientists to start Jupyter notebooks in its AWS accounts with the LEAST amount of operational overhead?

- A. Create a serverless front end using a static Amazon S3 website to allow the data scientists to request a Jupyter notebook instance by filling out a form. Use Amazon API Gateway to receive requests from the S3 website and trigger a central AWS Lambda function to make an API call to Amazon SageMaker that will launch a notebook instance with a preconfigured KMS key for the data scientists. Then call back to the front-end website to display the URL to the notebook instance.
- B. Create an AWS CloudFormation template to launch a Jupyter notebook instance using the AWS::SageMaker::NotebookInstance resource type with a preconfigured KMS key. Add a user-friendly name to the CloudFormation template. Display the URL to the notebook using the Outputs section. Distribute the CloudFormation template to the data scientists using a shared Amazon S3 bucket.
- C. Create an AWS CloudFormation template to launch a Jupyter notebook instance using the AWS::SageMaker::NotebookInstance resource type with a preconfigured KMS key. Simplify the parameter names, such as the instance size, by mapping them to Small, Large, and X-Large using the Mappings section in CloudFormation. Display the URL to the notebook using the Outputs section, then upload the template into an AWS Service Catalog product in the data scientist's portfolio, and share it with the data scientist's IAM role.
- D. Create an AWS CLI script that the data scientists can run locally. Provide step-by-step instructions about the parameters to be provided while executing the AWS CLI script to launch a Jupyter notebook with a preconfigured KMS key. Distribute the CLI script to the data scientists using a shared Amazon S3 bucket.

Commented [LC490]: https://aws.amazon.com/blogs/mt/enable-self-service-secured-data-science-using-amazon-sagemaker-notebooks-and-aws-service-catalog/

Question #792

What is the default maximum number of virtual private clouds (VPCs) per region?

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

Commented [LC491]: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html

Question #793

When setting your customer gateway to connect to your VPC, the _____ Association between the virtual private gateway and the customer gateway is formed first, utilizing the Pre-Shared Key as an authenticator.

- A. IPsec
- B. BGP
- C. IKE Security
- D. Tunnel

Commented [LC492]: C is the right answer.

https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html

https://en.wikipedia.org/wiki/Internet_Key_Exchange

Question #794

Which of the following is NOT a benefit of using Amazon Web Services 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.

Commented [LC493]: A is the right answer.

A: You need two DX to separate envs.
B: true
C: true
D: internet exchange rate is more expensive.

Ref. https://aws.amazon.com/getting-started/hands-on/connect-data-center-to-aws/services-costs/

Question #795

A business uses AWS CloudFormation as their application deployment tool. It stores all application binaries and templates in a versioned Amazon S3 bucket. The integrated development environment is hosted on an Amazon EC2 instance (IDE). After running the unit tests locally, the developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and publish the binaries to an S3 bucket. The developers want to enhance the current deployment method and to enable continuous integration and delivery (CI/CD) utilizing AWS CodePipeline.
The developers are looking for the following:
⇨ Use AWS CodeCommit for source control.
⇨ Automate unit testing and security scanning.
⇨ Alert the Developers when unit tests fail.
⇨ Turn application features on and off, and customize deployment dynamically as part of CI/CD.
⇨ Have the lead Developer provide approval before deploying an application.

Which solution will satisfy these criteria?

- A. Use AWS CodeBuild to run tests and security scans. Use an Amazon EventBridge rule to send Amazon SNS alerts to the Developers when unit tests fail. Write AWS Cloud Developer kit (AWS CDK) constructs for different solution features, and use a manifest file to turn features on and off in the AWS CDK application. Use a manual approval stage in the pipeline to allow the lead Developer to approve applications.
- B. Use AWS Lambda to run unit tests and security scans. Use Lambda in a subsequent stage in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Write AWS Amplify plugins for different solution features and utilize user prompts to turn features on and off. Use Amazon SES in the pipeline to allow the lead developer to approve applications.
- C. Use Jenkins to run unit tests and security scans. Use an Amazon EventBridge rule in the pipeline to send Amazon SES alerts to the developers when unit tests fail. Use AWS CloudFormation nested stacks for different solution features and parameters to turn features on and off. Use AWS Lambda in the pipeline to allow the lead developer to approve applications.
- D. Use AWS CodeDeploy to run unit tests and security scans. Use an Amazon CloudWatch alarm in the pipeline to send Amazon SNS alerts to the developers when unit tests fail. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use a manual approval stage in the pipeline to allow the lead developer to approve applications.

Commented [LC494]: A is the right answer.

B doesn't make sense.
C uses Jenkins which is not a AWS solution.
D doesn't convince because of Docker and CodeDeploy for testing and security scans.

Question #796

Who is responsible for updating the routing tables and networking ACLs in a VPC in order to guarantee that a database instance is available from other VPC instances?

- A. AWS administrators
- B. The owner of the AWS account
- C. Amazon
- D. The DB engine vendor

Commented [LC495]: 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.

Question #797

The Solutions Architect is responsible for implementing perimeter security protection while developing big applications on the AWS Cloud. AWS applications have the following endpoints:
⇨ Application Load Balancer
⇨ Amazon API Gateway regional endpoint
⇨ Elastic IP address-based EC2 instances.
⇨ Amazon S3 hosted websites.
⇨ Classic Load Balancer

The Solutions Architect is responsible for designing a solution that protects all of the web front ends stated above and includes the following security capabilities:
⇨ DDoS protection
⇨ SQL injection protection
⇨ IP address whitelist/blacklist
⇨ HTTP flood protection
⇨ Bad bot scraper protection

How should the solution be designed by the Solutions Architect?

- A. Deploy AWS WAF and AWS Shield Advanced on all web endpoints. Add AWS WAF rules to enforce the company's requirements.
- B. Deploy Amazon CloudFront in front of all the endpoints. The CloudFront distribution provides perimeter protection. Add AWS Lambda-based automation to provide additional security.
- C. Deploy Amazon CloudFront in front of all the endpoints. Deploy AWS WAF and AWS Shield Advanced. Add AWS WAF rules to enforce the company's requirements. Use AWS Lambda to automate and enhance the security posture.
- D. Secure the endpoints by using network ACLs and security groups and adding rules to enforce the company's requirements. Use AWS Lambda to automatically update the rules.

Commented [LC496]: C is the right answer. It is true that CLB is not supported with WAF but the CF distribution is indeed supported and you can use that endpoint.

Lambda can check the 3rd party IP reputation lists hourly for new ranges to block.

Question #798

Which of the following cannot be accomplished with the use of 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.

Commented [LC497]: It is C indeed.

Ref. https://aws.amazon.com/it/datapipeline/

Question #799

A business demands that all internal applications utilize private IP addresses for connection. A solutions architect has established interface endpoints to connect to AWS public services in order to accommodate this policy. The solutions architect observes that the service names resolve to public IP addresses and that internal services are unable to connect to the interface endpoints.

Which procedure should the solutions architect use in order to remedy this issue?

- A. Update the subnet route table with a route to the interface endpoint
- B. Enable the private DNS option on the VPC attributes
- C. Configure the security group on the interface endpoint to allow connectivity to the AWS services
- D. Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application

Commented [LC498]: B and C both look like valid answers.

B is correct over C referring to https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html#vpce-private-dns

Questions 800-827

Question #800

The application of a business is growing in popularity and suffering increased delay as a result of large volume reads on the database server.

The following properties apply to the service:

⇨ 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 organization wishes to minimize latency, improve in-region database read performance, and have multi-region disaster recovery capabilities capable of automatically performing a live recovery without data or performance loss (HA/DR).

Which deployment technique will satisfy these criteria?

- 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.

Commented [LC499]: Answer is A. Aurora read-replicas in the same and the DR region with an automatic failover capability (making the read-replica in the DR region the master upon DNS failover) is better than attempting to do the same with a customer managed solution on EC2 for SQL Server. Other options using ElasticCache do not provide automatic failover with no downtime.

Question #801

Which phase of the "get started with AWS Direct Connect" process tags the virtual interface you constructed with a customer-supplied tag that conforms with the Ethernet 802.1Q standard?

- A. Download Router Configuration.
- B. Complete the Cross Connect.
- C. Configure Redundant Connections with AWS Direct Connect.
- D. Create a Virtual Interface.

Commented [LC500]: D is the answer.

Ref.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/getting_started.html#createvirtualinterface

Question #802

A company's main office hosts a sizable on-premises MySQL database that supports an issue tracking system utilized by workers worldwide. The organization already utilizes AWS for some workloads and has configured an Amazon Route 53 entry for the database endpoint to refer to the on-premises database.
Management is worried about the database serving as a single point of failure and requests that a solutions architect relocate the database to AWS without causing data loss or downtime.

Which set of activities should be implemented by the solutions architect?

- A. Create an Amazon Aurora DB cluster. Use AWS Database Migration Service (AWS DMS) to do a full load from the on-premises database to Aurora. Update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
- B. During nonbusiness hours, shut down the on-premises database and create a backup. Restore this backup to an Amazon Aurora DB cluster. When the restoration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
- C. Create an Amazon Aurora DB cluster. Use AWS Database Migration Service (AWS DMS) to do a full load with continuous replication from the on-premises database to Aurora. When the migration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.
- D. Create a backup of the database and restore it to an Amazon Aurora multi-master cluster. This Aurora cluster will be in a master-master replication configuration with the on-premises database. Update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on- premises database.

Commented [LC501]: C is the answer: DMS + CDC is the winner.

Question #803

Which of the following Amazon RDS storage types is optimal for applications that need just light or burst I/O?

- A. Both magnetic and Provisioned IOPS storage
- B. Magnetic storage
- C. Provisioned IOPS storage
- D. None of these

Commented [LC502]: GP2 should be fine for light or burst I/O.

https://aws.amazon.com/ko/blogs/database/understanding-burst-vs-baseline-performance-with-amazon-rds-and-gp2/

Question #804

A business wants to use Amazon WorkSpaces to deliver desktop as a service (DaaS) to a number of workers. WorkSpaces will need authorisation to access files and services hosted on-premises depending on the company's Active Directory. The network will be connected using an existing AWS Direct Connect connection.

The answer must meet the following criteria:

⇨ Credentials from Active Directory should be used to access on-premises files and services.
⇨ Credentials from Active Directory should not be stored outside the company.
⇨ End users should have single sign-on (SSO) to on-premises files and services once connected to WorkSpaces.

Which authentication technique should the solutions architect employ for end users?

- A. Create an AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) directory within the WorkSpaces VPC. Use the Active Directory Migration Tool (ADMT) with the Password Export Server to copy users from the on-premises Active Directory to AWS Managed Microsoft AD. Set up a one- way trust allowing users from AWS Managed Microsoft AD to access resources in the on-premises Active Directory. Use AWS Managed Microsoft AD as the directory for WorkSpaces.
- B. Create a service account in the on-premises Active Directory with the required permissions. Create an AD Connector in AWS Directory Service to be deployed on premises using the service account to communicate with the on-premises Active Directory. Ensure the required TCP ports are open from the WorkSpaces VPC to the on-premises AD Connector. Use the AD Connector as the directory for WorkSpaces.
- C. Create a service account in the on-premises Active Directory with the required permissions. Create an AD Connector in AWS Directory Service within the WorkSpaces VPC using the service account to communicate with the on-premises Active Directory. Use the AD Connector as the directory for WorkSpaces.
- D. Create an AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) directory in the AWS Directory Service within the WorkSpaces VPC. Set up a one-way trust allowing users from the on-premises Active Directory to access resources in the AWS Managed Microsoft AD. Use AWS Managed Microsoft AD as the directory for WorkSpaces. Create an identity provider with AWS Identity and Access Management (IAM) from an on-premises ADFS server. Allow users from this identity provider to assume a role with a policy allowing them to run WorkSpaces.

Commented [LC503]: There's no need to "ensure the required TCP ports are open from the WS VPC to the on-prem AD Connector"

The connector is on aws, meaning B is wrong.

A is wrong, it violates 2nd req.

D is wrong because there's no need to create an additional AD on AWS.

C is the only feasible answer.

Question #805

An elastic network interface (ENI) is a virtual network interface that may be attached to a virtual private cloud (VPC) instance. An ENI may include a single public IP address, which is automatically allocated to the elastic network interface for eth0 when an instance is launched, but only when you _____ .

- A. create an elastic network interface for eth1
- B. include a MAC address
- C. use an existing network interface
- D. create an elastic network interface for eth0

Commented [LC504]: Should be the default action when you launch a EC2 instance

Question #806

A business is transferring its on-premises systems to Amazon Web Services (AWS). The following systems comprise the user environment:
⇨ Windows and Linux virtual machines running on VMware.
⇨ Physical servers running Red Hat Enterprise Linux.

Prior to shifting to AWS, the organization want to be able to complete the following steps:
⇨ Identify dependencies between on-premises systems.
⇨ Group systems together into applications to build migration plans.
⇨ Review performance data using Amazon Athena to ensure that Amazon EC2 instances are right-sized.

How are these stipulations to be met?

- A. Populate the AWS Application Discovery Service import template with information from an on-premises configuration management database (CMDB). Upload the completed import template to Amazon S3, then import the data into Application Discovery Service.
- B. Install the AWS Application Discovery Service Discovery Agent on each of the on-premises systems. Allow the Discovery Agent to collect data for a period of time.
- C. Install the AWS Application Discovery Service Discovery Connector on each of the on-premises systems and in VMware vCenter. Allow the Discovery Connector to collect data for one week.
- D. Install the AWS Application Discovery Service Discovery Agent on the physical on-premises servers. Install the AWS Application Discovery Service Discovery Connector in VMware vCenter. Allow the Discovery Agent to collect data for a period of time.

Commented [LC505]: Very tricky question. A and C are false and unfeasible.

D may be right as well as B. Although, the Connector gives less information than the agent solution, so, B is likely to be the correct one.

Also, the agent is for physical servers as well and not only virtual machines.

https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html#compare-tools

Question #807

A benefits enrollment firm hosts a three-tier web application on AWS in a VPC that contains a public Web tier NAT (Network Address Translation) instance. There is sufficient allocated capacity to handle the anticipated volume of work throughout the next fiscal year's benefit enrollment period, plus some additional overhead.
Enrollment proceeds normally for two days, at which point the web tier becomes unresponsive. Upon investigation using CloudWatch and other monitoring tools, it is discovered that an extremely large and unexpected amount of inbound traffic is 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 overburdened that administrators of benefit enrollment cannot even SSH into them.

Which action would be most effective in fighting off 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.

Commented [LC506]: B is too messy. C even more and SG do not have a deny rule. A is not feasible.

D is the solution. WAF may help as well in these situations.

Question #808

You've been hired as a solutions architect to help a business client migrate their e-commerce platform to Amazon Virtual Private Cloud (VPC)
The previous architect had previously implemented a three-tier virtual private cloud.
The following is the configuration:

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 prepared to begin provisioning EC2 instances inside the VPC. Web servers must have direct internet connectivity; application and database servers cannot.
Which of the following configurations enables remote administration of your application and database servers, as well as the ability for these servers to download 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.

Commented [LC507]: A is the right answer.

Question #809

With respect to Amazon SNS, you may send notification messages to mobile devices through any of the available push notification providers 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)

Commented [LC508]: 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. Reference: http://docs.aws.amazon.com/sns/latest/dg/SNSMobilePush.html

Question #810

Which of the following statements is correct about 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).

Commented [LC509]: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Question #811

A large corporation utilizes a multi-account AWS approach. Separate accounts are used to manage development staging and production workloads. The following criteria have been set to help manage expenses and enhance governance:

⇨ The company must be able to calculate the AWS costs for each project.
⇨ The company must be able to calculate the AWS costs for each environment development staging and production.
⇨ Commonly deployed IT services must be centrally managed.
⇨ Business units can deploy pre-approved IT services only.
⇨ Usage of AWS resources in the development account must be limited.

Which measures should be conducted in combination to achieve these requirements? (Select three.)

- A. Apply environment, cost center, and application name tags to all taggable resources.
- B. Configure custom budgets and define thresholds using Cost Explorer.
- C. Configure AWS Trusted Advisor to obtain weekly emails with cost-saving estimates.
- D. Create a portfolio for each business unit and add products to the portfolios using AWS CloudFormation in AWS Service Catalog.
- E. Configure a billing alarm in Amazon CloudWatch.
- F. Configure SCPs in AWS Organizations to allow services available using AWS.

Commented [LC510]: A, D, F
A - TAGS for cost management – ok
B - There is no requirement of budgeting
C - no requirement on cost saving or alerts
D - controlled provisioining – ok
E - no requirement of alarm
F - central - ok

Commented [LC511]:

Commented [LC512]:

Question #812

To guarantee that a table write happens, the specified throughput settings for the table and global secondary indexes in DynamoDB must be _____ ; otherwise, the table write 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

Commented [LC513]: A

Ref.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GSI.html

Question #813

Once a user has configured ElastiCache for an application and it is running, which services does Amazon not offer the user with:

- A. The ability for client programs to automatically identify all of the nodes in a cache cluster, and to initiate and maintain connections to all of these nodes
- B. Automating common administrative tasks such as failure detection and recovery, and software patching.
- C. Providing default Time to Live (TTL) in the AWS Elasticache Redis Implementation for different type of data.
- D. Providing detailed monitoring metrics associated with your Cache Nodes, enabling you to diagnose and react to issues very quickly

Commented [LC514]: C is the only one not included in the following ref:

https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/WhatIs.html

Question #814

The _____ service is intended for businesses with a large number of users or systems that make use of 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

Commented [LC515]:

Question #815

A load balancer is used to distribute traffic to Amazon EC2 instances contained inside a single Availability Zone. Security is an issue for the organization, and they want a solutions architect to re-build the system to fulfill the following requirements:

⇨ Inbound requests must be filtered for common vulnerability attacks.
⇨ Rejected requests must be sent to a third-party auditing application.
⇨ All resources should be highly available.

Which solution satisfies these criteria?

- A. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Use Amazon Inspector to monitor traffic to the ALB and EC2 instances. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.
- B. Configure an Application Load Balancer (ALB) and add the EC2 instances as targets. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.
- C. Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as targets. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.
- D. Configure a Multi-AZ Auto Scaling group using the application's AMI Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

Commented [LC516]: B, C should be out because they're not HA.

Between D, A I would pick A because D relies on the Marketplace

Question #816

Amazon S3 is used by a business to host a web application. The organization now employs a continuous integration tool running on an Amazon EC2 instance to create and deploy the application through an S3 bucket. A Solutions Architect is responsible for enhancing the platform's security in accordance with the following requirements:

⇨ A build process should be run in a separate account from the account hosting the web application.
⇨ A build process should have minimal access in the account it operates in.
⇨ Long-lived credentials should not be used.

To begin, the Development team built two AWS accounts: one for the application's web account process and another for the application's build account.

Which solution should the Solutions Architect implement in order to satisfy the security requirements?

- A. In the build account, create a new IAM role, which can be assumed by Amazon EC2 only. Attach the role to the EC2 instance running the continuous integration process. Create an IAM policy to allow s3: PutObject calls on the S3 bucket in the web account. In the web account, create an S3 bucket policy attached to the S3 bucket that allows the build account to use s3:PutObject calls.
- B. In the build account, create a new IAM role, which can be assumed by Amazon EC2 only. Attach the role to the EC2 instance running the continuous integration process. Create an IAM policy to allow s3: PutObject calls on the S3 bucket in the web account. In the web account, create an S3 bucket policy attached to the S3 bucket that allows the newly created IAM role to use s3:PutObject calls.
- C. In the build account, create a new IAM user. Store the access key and secret access key in AWS Secrets Manager. Modify the continuous integration process to perform a lookup of the IAM user credentials from Secrets Manager. Create an IAM policy to allow s3: PutObject calls on the S3 bucket in the web account, and attack it to the user. In the web account, create an S3 bucket policy attached to the S3 bucket that allows the newly created IAM user to use s3:PutObject calls.
- D. In the build account, modify the continuous integration process to perform a lookup of the IAM user credentials from AWS Secrets Manager. In the web account, create a new IAM user. Store the access key and secret access key in Secrets Manager. Attach the PowerUserAccess IAM policy to the IAM user.

Commented [LC517]: B is the solution.

C, D are unfeasible because they use long-lived credentials.

A is wrong because you allow a role to do something, not a account. You'd use a trust relationship in that case.

Question #817

You are in charge of a legacy web application whose server environment is nearing the end of its useful life. You want to transfer this program to AWS as soon as feasible, since the present environment of the application has the following limitations:

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

This is a mission-critical application with an RTO of 8 hours. 1-hour RPO (Recovery Point Objective).
How might you transfer this application to AWS in the most efficient manner while still adhering to your business continuity requirements?

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

Commented [LC518]: The answer is A.

See here: https://aws.amazon.com/de/blogs/aws/ec2-vm-import-connector/

B: EC2 VM Import/Export enables importing virtual machine (VM) images from existing virtualization environment to EC2, and then export them back EC2 VM Import/Export enables migration of applications and workloads to EC2, coping VM image catalog to EC2, or create a repository of VM images for backup and disaster recovery to leverage previous investments in building VMs by migrating your VMs to EC2. The supported file formats are: VMware ESX VMDK images, Citrix Xen VHD images, Microsoft Hyper-V VHD images, and RAW images For VMware vSphere, AWS Connector for vCenter can be used to export a VM from VMware and import it into Amazon EC2 For Microsoft Systems Center, AWS Systems Manager for Microsoft SCVMM can be used to import Windows VMs from SCVMM to EC2

Ref. https://aws.amazon.com/de/blogs/aws/ec2-vm-import-connector/

Question #818

A Solutions Architect has designed an AWS CloudFormation template for a three-tier application. The template includes an Auto Scaling group of Amazon EC2 instances running a custom AMI.
The Solutions Architect wants to guarantee that future upgrades to the custom AMI may be deployed to a running stack by first changing the template to refer to the new AMI and then performing UpdateStack to replace the EC2 instances with new AMI instances.

How can these needs be met via the deployment of AMI updates?

- A. Create a change set for a new version of the template, view the changes to the running EC2 instances to ensure that the AMI is correctly updated, and then execute the change set.
- B. Edit the AWS::AutoScaling::LaunchConfiguration resource in the template, changing its DeletionPolicy to Replace.
- C. Edit the AWS::AutoScaling::AutoScalingGroup resource in the template, inserting an UpdatePolicy attribute.
- D. Create a new stack from the updated template. Once it is successfully deployed, modify the DNS records to point to the new stack and delete the old stack.

Commented [LC519]: Should be C as per ref. https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-group-rolling-updates/

Question #819

You'd want to utilize AWS CodeDeploy to deploy an application to Amazon EC2 instances inside an Amazon Virtual Private Cloud (VPC).

Which criteria must be satisfied in order for something 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.)

Commented [LC520]: Answer is C.

Ref. https://aws.amazon.com/codedeploy/faqs/

Under "security"

Question #820

A business is transferring from on-premises to the AWS Cloud its three-tier web application. The following criteria apply to the migration process:

⇨ Ingest machine images from the on-premises environment.
⇨ Synchronize changes from the on-premises environment to the AWS environment until the production cutover.
⇨ Minimize downtime when executing the production cutover.
⇨ Migrate the virtual machines' root volumes and data volumes.

Which option will meet these criteria with the least amount of operational overhead?

- A. Use AWS Server Migration Service (SMS) to create and launch a replication job for each tier of the application. Launch instances from the AMIs created by AWS SMS. After initial testing, perform a final replication and create new instances from the updated AMIs.
- B. Create an AWS CLI VM Import/Export script to migrate each virtual machine. Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs created by VM Import/Export. Once testing is done, rerun the script to do a final import and launch the instances from the AMIs.
- C. Use AWS Server Migration Service (SMS) to upload the operating system volumes. Use the AWS CLI import-snapshot command for the data volumes. Launch instances from the AMIs created by AWS SMS and attach the data volumes to the instances. After initial testing, perform a final replication, launch new instances from the replicated AMIs, and attach the data volumes to the instances.
- D. Use AWS Application Discovery Service and AWS Migration Hub to group the virtual machines as an application. Use the AWS CLI VM Import/Export script to import the virtual machines as AMIs. Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs. After initial testing, perform a final virtual machine import and launch new instances from the AMIs.

Commented [LC521]: A allows to automate the migrations of machines as per requisites. B is too manual and C is with extra steps not needed. D is for other tasks.

Question #821

A financial services firm is migrating to AWS and wants to allow developers to experiment and innovate while restricting access to production apps.
The following conditions have been established by the company:
⇨ Production workloads cannot be directly connected to the internet.
⇨ All workloads must be restricted to the us-west-2 and eu-central-1 Regions.
⇨ Notification should be sent when developer sandboxes exceed $500 in AWS spending monthly.

Which combination of steps is required to develop a multi-account structure that fits the requirements of the business? (Select three.)

- A. Create accounts for each production workload within an organization in AWS Organizations. Place the production accounts within an organizational unit (OU). For each account, delete the default VPC. Create an SCP with a Deny rule for the attach an internet gateway and create a default VPC actions. Attach the SCP to the OU for the production accounts.
- B. Create accounts for each production workload within an organization in AWS Organizations. Place the production accounts within an organizational unit (OU). Create an SCP with a Deny rule on the attach an internet gateway action. Create an SCP with a Deny rule to prevent use of the default VPC. Attach the SCPs to the OU for the production accounts.
- C. Create a SCP containing a Deny Effect for cloudfront:*, iam:*, route53:*, and support:* with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the SCP to the organization's root.
- D. Create an IAM permission boundary containing a Deny Effect for cloudfront:*, iam:*, route53:*, and support:* with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the permission boundary to an IAM group containing the development and production users.
- E. Create accounts for each development workload within an organization in AWS Organizations. Place the development accounts within an organizational unit (OU). Create a custom AWS Config rule to deactivate all IAM users when an account's monthly bill exceeds $500.
- F. Create accounts for each development workload within an organization in AWS Organizations. Place the development accounts within an organizational unit (OU). Create a budget within AWS Budgets for each development account to monitor and report on monthly spending exceeding $500.

Commented [LC522]: Not completely convinced about this over A.

Commented [LC523]: C over D

Commented [LC524]: F over E

Question #822

A policy such as the one below may be linked to an IAM group. It enables an IAM user in that group to use the console to access a "home directory" on AWS S3 that matches their user-name.

```
{
    "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

Commented [LC525]: It's B because it misses the list all buckets: It still gives permission only to "my-company/home/${aws:username}/*" , Permission to list all buckets is necessary to navigate to this folder

Plus, the user wants to use the "console" to do it, so we can assume it's not a direct link to the folder.

Very useful reference: https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

"The ListAllMyBuckets action grants David permission to list all the buckets in the AWS account, which is required for navigating to buckets in the Amazon S3 console (and as an aside, you currently can't selectively filter out certain buckets, so users must have permission to list all buckets for console access). The console also does a GetBucketLocation call when users initially navigate to the Amazon S3 console, which is why David also requires permission for that action. Without these two actions, David will get an access denied error in the console."

Question #823

A manufacturing firm is expanding at a breakneck pace and has raised capital to upgrade its IT infrastructure and ecommerce presence. The company's ecommerce platform is comprised of the following:

⇨ Static assets primarily comprised of product images stored in Amazon S3.
⇨ Amazon DynamoDB tables that store product information, user information, and order information.
⇨ Web servers containing the application's front-end behind Elastic Load Balancers.

The corporation wishes to establish a disaster recovery facility in a distinct Region.

Which combination of activities should the solutions architect do in order to execute the new design while still adhering to all requirements? (Select three.)

- A. Enable Amazon Route 53 health checks to determine if the primary site is down, and route traffic to the disaster recovery site if there is an issue.
- B. Enable Amazon S3 cross-Region replication on the buckets that contain static assets.
- C. Enable multi-Region targets on the Elastic Load Balancer and target Amazon EC2 instances in both Regions.
- D. Enable DynamoDB global tables to achieve a multi-Region table replication.
- E. Enable Amazon CloudWatch and create CloudWatch alarms that route traffic to the disaster recovery site when application latency exceeds the desired threshold.
- F. Enable Amazon S3 versioning on the source and destination buckets containing static assets to ensure there is a rollback version available in the event of data corruption.

Commented [LC526]: This is how you route traffic. May be with a failover policy.

Commented [LC527]: If CRR is enabled then versioning is enabled meaning that F is wrong.

Commented [LC528]: That's how you enable DDB in multiple regions

Question #824

Which of the following is the Amazon Resource Name (ARN) condition operator that may be used in an Identity and Access Management (IAM) policy to ensure that the ARN is case-insensitive?

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

Commented [LC529]: The available arn operators are

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html

The only existing among the list is ArnLike

Question #825

Which of the following statements about the number of security groups and rules that apply to an EC2-Classic instance and an EC2-VPC network interface is correct?

- A. In EC2-Classic, you can associate an instance with up to 5 security groups and add up to 50 rules to a security group. In EC2-VPC, you can associate a network interface with up to 500 security groups and add up to 100 rules to a security group.
- B. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 50 rules to a security group. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 100 rules to a security group.
- C. In EC2-Classic, you can associate an instance with up to 5 security groups and add up to 100 rules to a security group. In EC2-VPC, you can associate a network interface with up to 500 security groups and add up to 50 rules to a security group.
- D. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 100 rules to a security group. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 50 rules to a security group.

Commented [LC530]: Outdated question?

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic. In EC2-Classic, you can associate an instance with up to 500 security groups and add up to 100 rules to a security group. If you're using EC2-VPC, you must use security groups created specifically for your VPC. In EC2-VPC, you can associate a network interface with up to 5 security groups and add up to 50 rules to a security group.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html#vpc-limits-security-groups

Question #826

Which combination of procedures may a Solutions Architect take to safeguard a web workload hosted on Amazon EC2 from DDoS and application layer attacks? (Choose two.)

- A. Put the EC2 instances behind a Network Load Balancer and configure AWS WAF on it.
- B. Migrate the DNS to Amazon Route 53 and use AWS Shield.
- C. Put the EC2 instances in an Auto Scaling group and configure AWS WAF on it.
- D. Create and use an Amazon CloudFront distribution and configure AWS WAF on it.
- E. Create and use an internet gateway in the VPC and use AWS Shield.

Commented [LC531]: AWS Shield Standard automatically protects your Amazon Route 53 Hosted Zones from infrastructure layer DDoS attacks"

https://aws.amazon.com/shield/?nc1=h_ls&whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Commented [LC532]: AWS WAF can be deployed on Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync.

https://aws.amazon.com/waf/faqs/

Question #827

Your supervisor has tasked you with the responsibility of developing an elastic network interface for each of your web servers that connects to a mid-tier network that houses an application server. Additionally, he wants to configure this as a Dual-homed Instance on Distinct Subnets.

Rather of routing network packets through the dual-homed instances, where should each dual-homed instance receive and process requests that satisfy his criteria?

- A. On one of the web servers
- B. On the front end
- C. On the back end
- D. Through a security group

Commented [LC533]: **Dual-homed** or **dual-homing** can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, one of the firewall architectures for implementing preventive security.
An example of dual-homed devices are enthusiast computing motherboards that incorporate dual Ethernet network interface cards.

Creating dual-homed instances with workloads/roles on distinct subnets
You can place a network interface on each of your web servers that connects to a mid-tier network where an application server resides. The application server can also be dual-homed to a backend network (subnet) where the database server resides. Instead of routing network packets through the dual-homed instances, each dual-homed instance receives and processes requests on the **front end**, initiates a connection to the backend, and then sends requests to the servers on the backend network.

Page 88: [1] Commented [LC277] Luca Cesarano 13/01/2022 21:34:00

ElastiCache for Memcached -

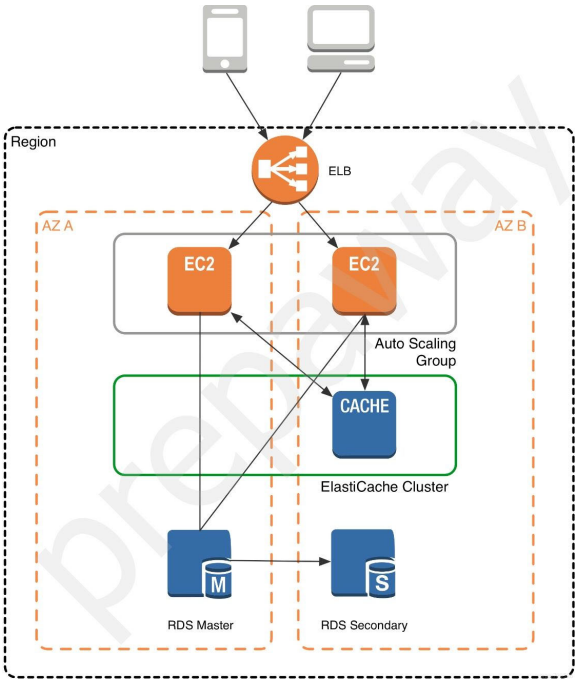
The primary goal of caching is typically to offload reads from your database or other primary data source. In most apps, you have hot spots of data that are regularly queried, but only updated periodically. Think of the front page of a blog or news site, or the top 100 leaderboard in an online game. 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 cachingfocused solution.

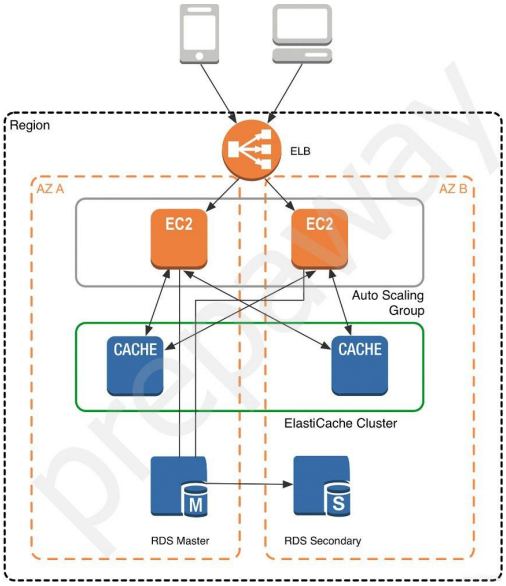
Architecture with ElastiCache for Memcached –

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:



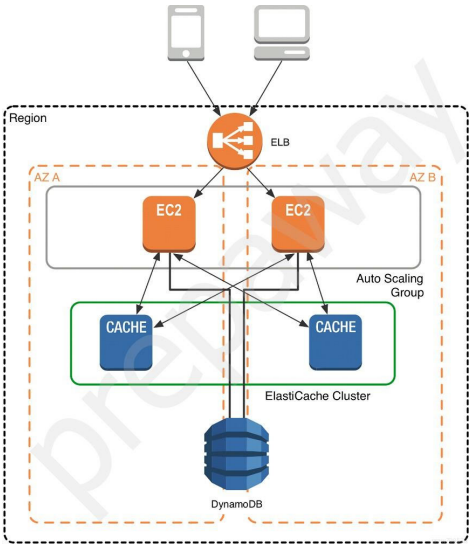
In this architecture diagram, the Amazon EC2 application instances are in an Auto Scaling group, located behind a load balancer using Elastic Load Balancing, which distributes requests among the instances. As requests come into a given EC2 instance, that EC2 instance is responsible for

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.

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.

Page 122: [2] Commented [LC395] Luca Cesarano 09/01/2022 16:24:00

B, D wrong.

A may be right, but C is correct.

An example policy to attach to the group:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "overrideBlockOnReq",
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": "ARN-OF-ROLE"
      },
      {
         "Sid": "limitedSize",
```

```
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
          "ForAnyValue:StringNotLike": {
            "ec2:InstanceType": [
              "*.nano",
              "*.small",
              "*.micro",
              "*.medium"
            ]
          }
        }
      }
    ]
}
```

Page 123: [3] Commented [LC400] Luca Cesarano 09/01/2022 16:02:00

CAREFUL, it says “UNNECESSARY” in the question.

The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web

Services (AWS) cloud. The user has complete control over the virtual networking environment. If the organization wants the Amazon EC2 instances to have a private IP address, he should create a public and private subnet for VPC in each Availability Zone (this is an AWS Elastic Beanstalk requirement). The organization should add their public resources, such as ELB and NAT to the public subnet, and AWC Elastic Beanstalk will assign them unique elastic IP addresses (a static, public IP address). The organization should launch Amazon EC2 instances in a private subnet so that AWS Elastic Beanstalk assigns them non-routable private IP addresses. Now the organization should configure route tables with the following rules:

☞ route all inbound traffic from ELB to EC2 instances

☞ route all outbound traffic from EC2 instances through NAT

Reference:

http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo-vpc.html