# SAP-C01 AWS-SAP AWS Certified Solutions Architect Professional

SAP-C01 Certified Solutions Architect Professional


英文名称：AWS Certified Solutions Architect Professional
科目代号：SAP-C01
中文名称：AWS 认证解决方案架构师-专业级
考试时间：190 分钟
考试题数：75 问
考题类型：单选题、多选题
通过成绩：75%
考试费用：300 USD [AWS-SAP 报名有优惠、可开发票]
证书期限：3 年有效期
考试语言： 英文、中文、日文、韩文
【题库只有英文原版题，报名考中文可以自己用有道词典翻译】

**AWS-C01.AWS-SAP**

**QUESTION 1**
A company runs a legacy system on a single m4.2xlarge Amazon EC2 instance with Amazon EBS2 storage. The EC2 instance runs both the web server and a self-managed Oracle database. A snapshot is made of the EBS volume every 12 hours, and an AMI was created from the fully configured EC2 instance. A recent event that terminated the EC2 instance led to several hours of downtime. The application was successfully launched from the AMI, but the age of the EBS snapshot and the repair of the database resulted in the loss of 8 hours of data. The system was also down for 4 hours while the Systems Operators manually performed these processes.
What architectural changes will minimize downtime and reduce the chance of lost data?

A. Create an Amazon CloudWatch alarm to automatically recover the instance. Create a script that will check and repair the database upon reboot. Subscribe the Operations team to the Amazon SNS message generated by 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 access multiple Availability Zones with a minimum instance count of one. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.
D. Increase the web server instance count to two m4.xlarge instances and use Amazon Route S3 round-robin load balancing to spread the load. Enable Route S3 health checks on the web servers. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Not highly available
C.One instance still not highly available
D.Route 53 don't have round-robin load balancing(may be weighting with 50/50?). Without auto scale it is not really scalable.



**QUESTION 2**
A Solutions Architect is working with a company that operates a standard three-tier web application in AWS. The web and application tiers run on Amazon EC2 and the database tier runs on Amazon RDS. The company is redesigning the web and application tiers to use Amazon API Gateway and AWS Lambda, and the company intends to deploy the new application within 6 months. The IT Manager has asked the Solutions Architect to reduce costs in the interim.
Which solution will be MOST cost effective while maintaining reliability?

A. Use Spot Instances for the web tier, On-Demand Instances for the application tier, and Reserved Instances for the database tier.
B. Use On-Demand Instances for the web and application tiers, and Reserved Instances for the database tier.
C. Use Spot Instances for the web and application tiers, and Reserved Instances for the database tier.
D. Use Reserved Instances for the web, application, and database tiers.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Spot instance can be interrupted
C.Spot instance can be interrupted
D.RI will need at least 1 year rental term, waste money after 6 month

**QUESTION 3**
A company uses Amazon S3 to store documents that may only be accessible to an Amazon EC2 instance in a certain virtual private cloud (VPC). The company fears that a malicious insider with access to this

instance could also set up an EC2 instance in another VPC to access these documents.
Which of the following solutions will provide the required protection?

A. Use an S3 VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint.
B. Use EC2 instance profiles and an S3 bucket policy to limit access to the role attached to the instance profile.
C. Use S3 client-side encryption and store the key in the instance metadata.
D. Use S3 server-side encryption and protect the key with an encryption context.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.The same role can be attached to another EC2 in another VPC
C.Instance metadata is not a safe place to store key
D.Other EC2 can use the same encryption context as well

**QUESTION 4**
The Solutions Architect manages a serverless application that consists of multiple API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables. Customers say that a few application components slow while loading dynamic images, and some are timing out with the "504 Gateway Timeout" error. While troubleshooting the scenario, the Solutions Architect confirms that DynamoDB monitoring metrics are at acceptable levels.
Which of the following steps would be optimal for debugging these application issues? (Choose two.)

A. Parse HTTP logs in Amazon API Gateway for HTTP errors to determine the root cause of the errors.
B. Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals.
C. Parse VPC Flow Logs to determine if there is packet loss between the Lambda function and S3.
D. Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors.
E. Parse S3 access logs to determine if objects being accessed are from specific IP addresses to narrow the scope to geographic latency issues.



**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.API gateway http log(cloudwatch) won't help with root cause
C.S3 is not VPC based (unless use vpc endpoint). Lambda could be VPC enabled, but not mentioned here.
E.Dynamic images are most likely go through a lambda function and S3 accessed by lambda should not have latency issues.

**QUESTION 5**
A Solutions Architect is designing the storage layer for a recently purchased application. The application will be running on Amazon EC2 instances and has the following layers and requirements:
* Data layer: A POSIX file system shared across many systems.
* Service layer: Static file content that requires block storage with more than 100k IOPS. Which combination of AWS services will meet these needs? (Choose two.)

A. Data layer - Amazon S3
B. Data layer - Amazon EC2 Ephemeral Storage
C. Data layer - Amazon EFS
D. Service layer - Amazon EBS volumes with Provisioned IOPS
E. Service layer - Amazon EC2 Ephemeral Storage

**Correct Answer:** CE
**Section: (none)**

**Explanation**

**Explanation/Reference:**
A.Not POSIX
B.Not persistent
D.Maximum EBS IOPS is 64000

**QUESTION 6**
A company has an application that runs a web service on Amazon EC2 instances and stores .jpg images in Amazon S3. The web traffic has a predictable baseline, but often demand spikes unpredictably for short periods of time. The application is loosely coupled and stateless. The .jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days, they are seldom accessed thereafter but always need to be immediately available.
The CIO has asked to find ways to reduce costs.
Which of the following options will reduce costs? (Choose two.)

A. Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes.
B. Configure a lifecycle policy to move the .jpg images on Amazon S3 to S3 IA after 30 days.
C. Use On-Demand instances for baseline capacity requirements and use Spot Fleet instances for the demand spikes.
D. Configure a lifecycle policy to move the .jpg images on Amazon S3 to Amazon Glacier after 30 days.
E. Create a script that checks the load on all web servers and terminates unnecessary On-Demand instances.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**
C.Spot instance for spike is not good as spot can be interrupted
D.Glacier can take up to hours to access data
E.Should use auto scale group

**QUESTION 7**
A hybrid network architecture must be used during a company's multi-year data center migration from multiple private data centers to AWS. The current data centers are linked together with private fiber. Due to unique legacy applications, NAT cannot be used. During the migration period, many applications will need access to other applications in both the data centers and AWS.
Which option offers a hybrid network architecture that is secure and highly available, that allows for high bandwidth and a multi-region deployment post-migration?

A. Use AWS Direct Connect to each data center from different ISPs, and configure routing to failover to the other data center's Direct Connect if one fails. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.
B. Use multiple hardware VPN connections to AWS from the on-premises data center. Route different subnet traffic through different VPN connections. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.
C. Use a software VPN with clustering both in AWS and the on-premises data center, and route traffic through the cluster. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.
D. Use AWS Direct Connect and a VPN as backup, and configure both to use the same virtual private gateway and BGP. Ensure that no VPC CIDR blocks overlap one another or the on-premises network.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B. is not high bandwidth
C.One VPN connection is not HA (cluster still have one connection)
D.As a backup, VPN is not sufficient with high bandwidth. Also, what if the region that have the virtual private gateway fails?

**QUESTION 8**
A company is currently running a production workload on AWS that is very I/O intensive. Its workload consists of a single tier with 10 c4.8xlarge instances, each with 2 TB gp2 volumes. The number of processing jobs has recently increased, and latency has increased as well. The team realizes that they are constrained on the IOPS. For the application to perform efficiently, they need to increase the IOPS by 3,000 for each of the instances.
Which of the following designs will meet the performance goal MOST cost effectively?

A. Change the type of Amazon EBS volume from gp2 to io1 and set provisioned IOPS to 9,000.
B. Increase the size of the gp2 volumes in each instance to 3 TB.
C. Create a new Amazon EFS file system and move all the data to this new file system. Mount this file system to all 10 instances.
D. Create a new Amazon S3 bucket and move all the data to this new bucket. Allow each instance to access this S3 bucket and use it for storage.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Cost will be 3000 * 0.125 + 9000 * 0.065
B.Cost will be 3000 * 0.1 (gp2 has 3 IOPS per GB)
C.EFS has higher latency than EBS provisioned IOPS (https://docs.aws.amazon.com/efs/latest/ug/performance.html)
D.S3 won't be as fast as EBS in terms of IO

**QUESTION 9**
A company's data center is connected to the AWS Cloud over a minimally used 10-Gbps AWS Direct Connect connection with a private virtual interface to its virtual private cloud (VPC). The company internet connection is 200 Mbps, and the company has a 150-TB dataset that is created each Friday. The data must be transferred and available in Amazon S3 on Monday morning.
Which is the LEAST expensive way to meet the requirements while allowing for data transfer growth?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Won't be fast enough (courier on the weekend?~!)
B.S3 VPC endpoint is Gateway Endpoint and it cannot extend across direct connect
https://docs.amazonaws.cn/en_us/vpc/latest/userguide/vpce-gateway.html#Gateway-Endpoint-Limitations
C.Proxy farm is more expensive than D

**QUESTION 10**
A company has created an account for individual Development teams, resulting in a total of 200 accounts. All accounts have a single virtual private cloud (VPC) in a single region with multiple microservices running in Docker containers that need to communicate with microservices in other accounts. The Security team requirements state that these microservices must not traverse the public internet, and only certain internal services should be allowed to call other individual services. If there is any denied network traffic for a service, the Security team must be notified of any denied requests, including the source IP. How can connectivity be established between service while meeting the security requirements?

A. Create a VPC peering connection between the VPCs. Use security groups on the instances to allow traffic from the security group IDs that are permitted to call the microservice. Apply network ACLs to and allow traffic from the 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 on the other accounts. Enable VPC Flow Logs, and use an Amazon CloudWatch Logs subscription filter for rejected traffic. Create an IAM role and allow the Security team to call the AssumeRole action for each account.

C. Deploy a transit VPC by using third-party marketplace VPN appliances running on Amazon EC2, dynamically routed VPN connections between the VPN appliance, and the virtual private gateways (VGWs) attached to each VPC 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 the allowed services. Create VPC Flow Logs on each VPC to capture rejected traffic that will be delivered to an Amazon CloudWatch Logs group. Create a CloudWatch Logs subscription that streams the log data to a security account.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.HTTP 403 won't be denied requests as the request will never get to ECS
VPC peering will maintain the original IP (therefore no CIDR overlap is allowed)
B.Log in multiple account is not best practice. Moreover, if only one of two services in a VPC should access a particular micro service, this won't work as the SG allow the whole VPC
VPN will keep the original IP, unless NAT is used before traffic going into the tunnel
C.All traffic go to the same VPN appliance which means cannot actually block service access. ACLs allow local VPC only, than the transit VPC will not work.
D.This will not work as PrivateLink will create a service endpoint with the local VPC's private IP, which means you will not have the source IP, and the security group in the producer cannot range the allowed services.
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-privatelink.html
However, when a service is rejected on the consumer VPC, a log should have the source IP for the VPC endpoint. However, the allowed IP on the producer side is tricky. I think it means the allowed service within the same VPC. Anyway, I think this is the only solution that make sense, even though there is a lot of vague description in it

**QUESTION 11**
A company runs a dynamic mission-critical web application that has an SLA of 99.99%. Global application users access the application 24/7. The application is currently hosted on premises and routinely fails to meet its SLA, especially when millions of users access the application concurrently. Remote users complain of latency. How should this application be redesigned to be scalable and allow for automatic failover at the lowest cost?

A. Use Amazon Route 53 failover routing with geolocation-based routing. Host the website on automatically scaled Amazon EC2 instances behind an Application Load Balancer with an additional Application Load Balancer and EC2 instances for the application layer in each region. Use a Multi-AZ deployment with MySQL as the data layer.

B. Use Amazon Route 53 round robin routing to distribute the load evenly to several regions with health checks. Host the website on automatically scaled Amazon ECS with AWS Fargate technology containers behind a Network Load Balancer, with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora replicas for the data layer.

C. Use Amazon Route 53 latency-based routing to route to the nearest region with health checks. Host the website in Amazon S3 in each region and use Amazon API Gateway with AWS Lambda for the application layer. Use Amazon DynamoDB global tables as the data layer with Amazon DynamoDB Accelerator (DAX) for caching.
D. Use Amazon Route 53 geolocation-based routing. Host the website on automatically scaled AWS argate containers behind a Network Load Balancer with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora Multi-Master for Aurora MySQL as the data layer.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will be more expensive than C
B.Route 53 round robin routing is not a thing
NLB do not support sticky session and web application most likely will need one
C.Using managed service is the best practice. S3, Lambda and DynamoDB is so much cheaper than EC2 and RDS
D.Sticky session not supported in NLB, and Multi Master cannot cross region

**QUESTION 12**
A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in a single AWS Region The fully qualified domain names (FQDNs) of all of the applications are made available through HTTPS using Application Load Balancers (ALBs). The ALBs are configured to use public SSL/TLS certificates. A Solutions Architect needs to migrate the web applications to a multi-region architecture. All HTTPS services should continue to work without interruption.
Which approach meets these requirements?

A. Request a certificate for each FQDN using AWS KMS. Associate the certificates with the ALBs in the primary AWS Region. Enable cross-region availability in AWS KMS for the certificates and associate the certificates with the ALBs in the secondary AWS Region.
B. Generate the key pairs and certificate requests for each FQDN using AWS KMS. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
C. Request a certificate for each FQDN using AWS Certificate Manager. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.
D. Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manager. Associate the certificates with the corresponding ALBs in each AWS Region.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
71
A.KMS is not for certificate
B.KMS is not for certificate
C.Certificates for ELB cannot be cross region
https://aws.amazon.com/certificate-manager/faqs/

**QUESTION 13**
An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a Solutions Architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays. Which of the following is the MOST reliable approach to meet the requirements?

A. Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.
B. Receive the orders in an Amazon SQS queue and trigger an AWS Lambda function to process them.

C. Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container to process them.
D. Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Really bad...
B.Lambda function is more reliable and scalable
C.This is not what step function is for
D.Need to config auto scale, and kinesis do not have item level ack

**QUESTION 14**
A company has an application written using an in-house software framework. The framework installation takes 30 minutes and is performed with a user data script. Company Developers deploy changes to the application frequently. The framework installation is becoming a bottleneck in this process.
Which of the following would speed up this process?

A. Create a pipeline to build a custom AMI with the framework installed and use this AMI as a baseline for application deployments.
B. Employ a user data script to install the framework but compress the installation files to make them smaller.
C. Create a pipeline to parallelize the installation tasks and call this pipeline from a user data script.
D. Configure an AWS OpsWorks cookbook that installs the framework instead of employing user data. Use this cookbook as a base for all deployments.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Installation cannot be parallelized...
C.Installation cannot be parallelized...
D.Cookbook is a collection of receipts, I think it should be receipt here. However, this still need to run the installation and won't shorter the time

**QUESTION 15**
A company wants to ensure that the workloads for each of its business units have complete autonomy and a minimal blast radius in AWS. The Security team must be able to control access to the resources and services in the account to ensure that particular services are not used by the business units.
How can a Solutions Architect achieve the isolation requirements?

A. Create individual accounts for each business unit and add the account to an OU in AWS Organizations. Modify the OU to ensure that the particular services are blocked. Federate each account with an IdP, and create separate roles for the business units and the Security team.
B. Create individual accounts for each business unit. Federate each account with an IdP and create separate roles and policies for business units and the Security team.
C. Create one shared account for the entire company. Create separate VPCs for each business unit. Create individual IAM policies and resource tags for each business unit.
Federate each account with an IdP, and create separate roles for the business units and the Security team.
D. Create one shared account for the entire company. Create individual IAM policies and resource tags for each business unit. Federate the account with an IdP, and create separate roles for the business units and the Security team.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Best practice with minimal blast radius and autonomy
B.

**QUESTION 16**
A company is migrating a subset of its application APIs from Amazon EC2 instances to run on a serverless infrastructure. The company has set up Amazon API Gateway, AWS Lambda, and Amazon DynamoDB for the new application. The primary responsibility of the Lambda function is to obtain data from a third-party Software as a Service (SaaS) provider. For consistency, the Lambda function is attached to the same virtual private cloud (VPC) as the original EC2 instances. Test users report an inability to use this newly moved functionality, and the company is receiving 5xx errors from API Gateway. Monitoring reports from the SaaS provider shows that the requests never made it to its systems. The company notices that Amazon CloudWatch Logs are being generated by the Lambda functions. When the same functionality is tested against the EC2 systems, it works as expected What is causing the issue?

A. Lambda is in a subnet that does not have a NAT gateway attached to it to connect to the SaaS provider.
B. The end-user application is misconfigured to continue using the endpoint backed by EC2 instances.
C. The throttle limit set on API Gateway is too low and the requests are not making their way through.
D. API Gateway does not have the necessary permissions to invoke Lambda.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.There is Lambda logs
C.If this is the case, some of the request will work
D.There is lambda logs

**QUESTION 17**
A Solutions Architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month.
Which combination of steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Choose three.)

A. Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances.
B. Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types.
C. Purchase all upfront Reserved Instances that cover 100% of the account's expected Amazon EC2 usage.
D. Place conditions in the users' IAM policies that limit the number of instances they are able to launch.
E. Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console.
F. Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost.

**Correct Answer:** AEF
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.aws:RequestTag/tag-key
B.Bad practice
C.Not going to work as this may ends up cost more
D.IAM do not support this
https://forums.aws.amazon.com/thread.jspa?threadID=174503
E.
F.

**QUESTION 18**
A large global company wants to migrate a stateless mission-critical application to AWS. The application is based on IBM WebSphere (application and integration middleware), IBM MQ (messaging middleware), and

IBM DB2 (database software) on a z/OS operating system.
How should the Solutions Architect migrate the application to AWS?

A. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM MQ to an Amazon EC2-based MQ. Re-platform the z/OS-based DB2 to Amazon RDS DB2.
B. Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling.Re-platform the IBM MQ to an Amazon MQ. Re-platform z/OS-based DB2 to Amazon EC2-based DB2.
C. Orchestrate and deploy the application by using AWS Elastic Beanstalk. Re-platform the IBM MQ to Amazon SQS. Re-platform z/OS-based DB2 to Amazon RDS DB2.
D. Use the AWS Server Migration Service to migrate the IBM WebSphere and IBM DB2 to an Amazon EC2-based solution. Re-platform the IBM MQ to an Amazon MQ.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.RDS does not support DB2
B.
C.RDS does not support DB2
D.Server MIgration Service works with VM and nothing about VM is mentioned, SMS only support Linux and windows
https://docs.aws.amazon.com/server-migration-service/latest/userguide/prereqs.html#os_prereqs

**QUESTION 19**
A media storage application uploads user photos to Amazon S3 for processing. End users are reporting that some uploaded photos are not being processed properly. The Application Developers trace the logs and find that AWS Lambda is experiencing execution issues when thousands of users are on the system simultaneously. Issues are caused by:
* Limits around concurrent executions.
* The performance of Amazon DynamoDB when saving data. Which actions can be taken to increase the performance and reliability of the application? (Choose two.)

A. Evaluate and adjust the read capacity units (RCUs) for the DynamoDB tables.
B. Evaluate and adjust the write capacity units (WCUs) for the DynamoDB tables.
C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions
D. Configure a dead letter queue that will reprocess failed or timed-out Lambda functions.
E. Use S3 Transfer Acceleration to provide lower-latency access to end users.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
A company operates a group of imaging satellites. The satellites stream data to one of the company's ground stations where processing creates about 5 GB of images per minute. This data is added to network-attached storage, where 2 PB of data are already stored.
The company runs a website that allows its customers to access and purchase the images over the Internet. This website is also running in the ground station. Usage analysis shows that customers are most likely to access images that have been captured in the last 24 hours. The company would like to migrate the image storage and distribution system to AWS to reduce costs and increase the number of customers that can be served. Which AWS architecture and migration strategy will meet these requirements?

A. Use multiple AWS Snowball appliances to migrate the existing imagery to Amazon S3.
Create a 1-Gb AWS Direct Connect connection from the ground station to AWS, and upload new data to Amazon S3 through the Direct Connect connection. Migrate the data distribution website to Amazon EC2 instances. By using Amazon S3 as an origin, have this website serve the data through Amazon

CloudFront by creating signed URLs.

B. Create a 1-Gb Direct Connect connection from the ground station to AWS. Use the AWS Command Line Interface to copy the existing data and upload new data to Amazon S3 over the Direct Connect connection. Migrate the data distribution website to EC2 instances. By using Amazon S3 as an origin, have this website serve the data through CloudFront by creating signed URLs.

C. Use multiple Snowball appliances to migrate the existing images to Amazon S3. Upload new data by regularly using Snowball appliances to upload data from the network-attached storage. Migrate the data distribution website to EC2 instances. By using Amazon S3 as an origin, have this website serve the data through CloudFront by creating signed URLs.

D. Use multiple Snowball appliances to migrate the existing images to an Amazon EFS file system. Create a 1-Gb Direct Connect connection from the ground station to AWS, and upload new data by mounting the EFS file system over the Direct Connect connection.
Migrate the data distribution website to EC2 instances. By using webservers in EC2 that mount the EFS file system as the origin, have this website serve the data through CloudFront by creating signed URLs.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.
B.1GB for 2PB will be too slow
C.Snowball cannot ensure data is available for last 24 hour
D.EFS is expensive in this case

**QUESTION 21**
A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics is run, and each execution takes about 4 hours to complete. The statistical analysis is not mission critical to the business, and previous data points are picked up on the next execution if a particular run fails. The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations running full time to ingest and store the streaming data in attached Amazon EBS volumes. On-Demand EC2 instances are launched each night to perform the nightly processing, accessing the stored data from NFS shares on the ingestion servers, and terminating the nightly processing servers when complete. The Reserved Instance reservations are expiring, and the company needs to determine whether to purchase new reservations or implement a new design.
Which is the most cost-effective design?

A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a fleet of On-Demand EC2 instances that launches each night to perform the batch processing of the S3 data and terminates when the processing completes.

B. Update the ingestion process to use Amazon Kinesis Data Firehouse to save data to Amazon S3. Use AWS Batch to perform nightly processing with a Spot market bid of 50% of the On-Demand price.

C. Update the ingestion process to use a fleet of EC2 Reserved Instances behind a Network Load Balancer with 3-year leases. Use Batch with Spot instances with a maximum bid of 50% of the On-Demand price for the nightly processing.

D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon Redshift. Use an AWS Lambda function scheduled to run nightly with Amazon CloudWatch Events to query Amazon Redshift to generate the daily statistics.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.More expensive than B
B.As it is not mission critical and can pick up from previous data point, Spot instance makes sense
C.If we still use EBS, each instance will have its own EBS and data is hard to aggregate. EC2 is expensive as well
D.Lambda has process limit of 15 mins

**QUESTION 22**
A three-tier web application runs on Amazon EC2 instances. Cron daemons are used to trigger scripts that

collect the web server, application, and database logs and send them to a centralized location every hour. Occasionally, scaling events or unplanned outages have caused the instances to stop before the latest logs were collected, and the log files were lost. Which of the following options is the MOST reliable way of collecting and preserving the log files?

A. Update the cron to run every 5 minutes instead of every hour to reduce the possibility of log messages being lost in an outage.
B. Use Amazon CloudWatch Events to trigger Amazon Systems Manager Run Command to invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage.
C. Use the Amazon CloudWatch Logs agent to stream log messages directly to CloudWatch Logs. Configure the agent with a batch count of 1 to reduce the possibility of log messages being lost in an outage.
D. Use Amazon CloudWatch Events to trigger AWS Lambda to SSH into each running instance and invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Almost no delay. Most reliable

**QUESTION 23**
A company stores sales transaction data in Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes to the items stored in the DynamoDB tables must be logged within 30 minutes.
Which solution meets the requirements?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.We want to track item changes, not table changes
C.Best practice
D.DynamoDB is not supported by cloudwatch events, you will need cloudtrail

**QUESTION 24**
A company is running multiple applications on Amazon EC2. Each application is deployed and managed by multiple business units. All applications are deployed on a single AWS account but on different virtual private clouds (VPCs). The company uses a separate VPC in the same account for test and development purposes. Production applications suffered multiple outages when users accidentally terminated and modified resources that belonged to another business unit. A Solutions Architect has been asked to improve the availability of the company applications while allowing the Developers access to the resources they need.
Which option meets the requirements with the LEAST disruption?

A. Create an AWS account for each business unit. Move each business unit's instances to its own account and set up a federation to allow users to access their business unit's account.

B. Set up a federation to allow users to use their corporate credentials, and lock the users down to their own VPC. Use a network ACL to block each VPC from accessing other VPCs.
C. Implement a tagging policy based on business units. Create an IAM policy so that each user can terminate instances belonging to their own business units only.
D. Set up role-based access for each user and provide limited permissions based on individual roles and the services for which each user is responsible.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Move instance across account lead to interruption
B.Will stop inter service communication
C.Develop and test instances won't be catered for

**QUESTION 25**
An enterprise runs 103 line-of-business applications on virtual machines in an onpremises data center. Many of the applications are simple PHP, Java, or Ruby web applications, are no longer actively developed, and serve little traffic. Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs?

A. Deploy the applications to single-instance AWS Elastic Beanstalk environments without a load balancer.
B. Use AWS SMS to create AMIs for each virtual machine and run them in Amazon EC2.
C. Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.
D. Use VM Import/Export to create AMIs for each virtual machine and run them in single-instance AWS Elastic Beanstalk environments by configuring a custom image.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.103 EC2 still needed
B.103 EC2
C.We could run all ECS container in one small EC2 and use ALB to route, which can be really cheap
D.103 EC2



**QUESTION 26**
A Solutions Architect must create a cost-effective backup solution for a company's 500MB source code repository of proprietary and sensitive applications. The repository runs on Linux and backs up daily to tape. Tape backups are stored for 1 year. The current solutions are not meeting the company's needs because it is a manual process that is prone to error, expensive to maintain, and does not meet the need for a Recovery Point Objective (RPO) of 1 hour or Recovery Time Objective (RTO) of 2 hours. The new disaster recovery requirement is for backups to be stored offsite and to be able to restore a single file if needed. Which solution meets the customer's needs for RTO, RPO, and disaster recovery with the LEAST effort and expense?

A. Replace local tapes with an AWS Storage Gateway virtual tape library to integrate with current backup software. Run backups nightly and store the virtual tapes on Amazon S3 standard storage in US-EAST-1. Use cross-region replication to create a second copy in US-WEST-2. Use Amazon S3 lifecycle policies to perform automatic migration to Amazon Glacier and deletion of expired backups after 1 year?
B. Configure the local source code repository to synchronize files to an AWS Storage Gateway file Amazon gateway to store backup copies in an Amazon S3 Standard bucket.
Enable versioning on the Amazon S3 bucket. Create Amazon S3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard 0 Infrequent Access, then Amazon Glacier, then delete backups after 1 year.
C. Replace the local source code repository storage with a Storage Gateway stored volume.
Change the default snapshot frequency to 1 hour. Use Amazon S3 lifecycle policies to archive snapshots to Amazon Glacier and remove 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 on hourly AWS Lambda task to copy snapshots from US-EAST -1 to US-WEST-2.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Cannot meet RPO of 1 hour
C.Volume gateway store a snapshot, which doesn't allow restore of single file
https://aws.amazon.com/storagegateway/faqs

**QUESTION 27**
A company CFO recently analyzed the company's AWS monthly bill and identified an opportunity to reduce the cost for AWS Elastic Beanstalk environments in use. The CFO has asked a Solutions Architect to design a highly available solution that will spin up an Elastic Beanstalk environment in the morning and terminate it at the end of the day. The solution should be designed with minimal operational overhead and to minimize costs. It should also be able to handle the increased use of Elastic Beanstalk environments among different teams, and must provide a one-stop scheduler solution for all teams to keep the operational costs low.
What design will meet these requirements?

A. Set up a Linux EC2 Micro instance. Configure an IAM role to allow the start and stop of the Elastic Beanstalk environment and attach it to the instance. Create scripts on the instance to start and stop the Elastic Beanstalk environment. Configure cron jobs on the instance to execute the scripts.
B. Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution role granting Elastic Beanstalk environment start/stop permissions, and assign the role to the Lambda functions. Configure cron expression Amazon CloudWatch Events rules to trigger the Lambda functions.
C. Develop an AWS Step Functions state machine with "wait" as its type to control the start and stop time. Use the activity task to start and stop the Elastic Beanstalk environment. Create a role for Step Functions to allow it to start and 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 date. At the end of the day, scale down the instance number to 0 to terminate the EC2 instance.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Need to have an EC2 running all the time
B.Recommended solution
https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/
C.Step function is not used for this, and the role with step function will not help the worker task.
D.EC2 need to run during datetime..and not really good solution

**QUESTION 28**
A company plans to move regulated and security-sensitive businesses to AWS. The Security team is developing a framework to validate the adoption of AWS best practice and industryrecognized compliance standards. The AWS Management Console is the preferred method for teams to provision resources.
Which strategies should a Solutions Architect use to meet the business requirements and continuously assess, audit, and monitor the configurations of AWS resources? (Choose two.)

A. Use AWS Config rules to periodically audit changes to AWS resources and monitor the compliance of the configuration. Develop AWS Config custom rules using AWS Lambda to establish a testdriven 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 machines 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.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.
B.Management Console do not go through SDK
C.
D.Need cloudtrail to log resource change to cloudwatch
E.Cloudtrail to SNS has no filtering so you will need to send all the logs.
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html#configure-cloudtrail-to-send-notifications

**QUESTION 29**
A company is running a high-user-volume media-sharing application on premises. It currently hosts about 400 TB of data with millions of video files. The company is migrating this application to AWS to improve reliability and reduce costs. The Solutions Architecture team plans to store the videos in an Amazon S3 bucket and use Amazon CloudFront to distribute videos to users. The company needs to migrate this application to AWS 10 days with the least amount of downtime possible. The company currently has 1 Gbps connectivity to the Internet with 30 percent free capacity.
Which of the following solutions would enable the company to migrate the workload to AWS and meet all of the requirements?

A. Use a multi-part upload in Amazon S3 client to parallel-upload the data to the Amazon S3 bucket over the Internet. Use the throttling feature to ensure that the Amazon S3 client does not use more than 30 percent of available 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.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Takes 123 day…. Parralel still have the internet connection as bottleneck
B.Snowmobile is recommended for more than 10PB
C.Takes 123 days...

**QUESTION 30**
A company has developed a new billing application that will be released in two weeks. Developers are

testing the application running on 10 EC2 instances managed by an Auto Scaling group in subnet 172.31.0.0/24 within VPC A with CIDR block 172.31.0.0/16. The Developers noticed connection timeout errors in the application logs while connecting to an Oracle database running on an Amazon EC2 instance in the same region within VPC B with CIDR block 172.50.0.0/16. The IP of the database instance is hard-coded in the application instances.
Which recommendations should a Solutions Architect present to the Developers to solve the problem in a secure way with minimal maintenance and overhead?

A. Disable the SrcDestCheck attribute for all instances running the application and Oracle Database. Change the default route of VPC A to point ENI of the Oracle Database that has an IP address assigned within the range of 172.50.0.0/26
B. Create and attach internet gateways for both VPCs. Configure default routes to the Internet gateways for both VPCs. Assign an Elastic IP for each Amazon EC2 instance in VPC A
C. Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 172.50.0.0/16
D. Create an additional Amazon EC2 instance for each VPC as a customer gateway; create one virtual private gateway (VGW) for each VPC, configure an end-to-end VPC, and advertise the routes for 172.50.0.0/16

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This is for NAT? And it is not going to help as the destination is the database and the source will be the EC2s
B.Database connection should not go through internet
D.Transit VPC is too much a trouble!

**QUESTION 31**
A Solutions Architect has been asked to look at a company's Amazon Redshift cluster, which has quickly become an integral part of its technology and supports key business process. The Solutions Architect is to increase the reliability and availability of the cluster and provide options to ensure that if an issue arises, the cluster can either operate or be restored within four hours.
Which of the following solution options BEST addresses the business need in the most costeffective manner?

A. Ensure that the Amazon Redshift cluster has been set up to make use of Auto Scaling groups with the nodes in the cluster spread across multiple Availability Zones.
B. Ensure that the Amazon Redshift cluster creation has been template using AWS CloudFormation so it can easily be launched in another Availability Zone and data populated from the automated Redshift back-ups stored in Amazon S3.
C. Use Amazon Kinesis Data Firehose to collect the data ahead of ingestion into Amazon Redshift and create clusters using AWS CloudFormation in another region and stream the data to both clusters.
D. Create two identical Amazon Redshift clusters in different regions (one as the primary, one as the secondary). Use Amazon S3 cross-region replication from the primary to secondary). Use Amazon S3 cross-region replication from the primary to secondary region, which triggers an AWS Lambda function to populate the cluster in the secondary region.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Redshift cluster is single AZ…
https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-clusters.html#az-considerations
B.Best practice
C.We have 4 hour RPO so we don't need a redundant cluster
D.Not making sense, and lambda probably time out….

**QUESTION 32**
A company prefers to limit running Amazon EC2 instances to those that were launched from AMIs pre-

approved by the Information Security department. The Development team has an agile continuous integration and deployment process that cannot be stalled by the solution.
Which method enforces the required controls with the LEAST impact on the development process? (Choose two.)

A. Use IAM policies to restrict the ability of users or other automated entities to launch EC2 instances based on a specific set of pre-approved AMIs, such as those tagged in a specific way by Information Security.
B. Use regular scans within Amazon Inspector with a custom assessment template to determine if the EC2 instance that the Amazon Inspector Agent is running on is based upon a pre-approved AMI. If it is not, shut down the instance and inform information Security by email that this occurred.
C. Only allow launching of EC2 instances using a centralized DevOps team, which is given work packages via notifications from an internal ticketing system. Users make requests for resources using this ticketing tool, which has manual information security approval steps to ensure that EC2 instances are only launched from approved AMIs.
D. Use AWS Config rules to spot any launches of EC2 instances based on non-approved AMIs, trigger an AWS Lambda function to automatically terminate the instance, and publish a message to an Amazon SNS topic to inform Information Security that this occurred.
E. Use a scheduled AWS Lambda function to scan through the list of running instances within the virtual private cloud (VPC) and determine if any of these are based on unapproved AMIs.
Publish a message to an SNS topic to inform Information Security that this occurred and then shut down the instance.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.AWS inspector is used to find security vulnerability, not used to find AMI
C.Not agile…
E.Scheduled lambda is not a thing, you need cloudwatch event to trigger Lambda

**QUESTION 33**
A Company has a security event whereby an Amazon S3 bucket with sensitive information was made public. Company policy is to never have public S3 objects, and the Compliance team must be informed immediately when any public objects are identified. How can the presence of a public S3 object be detected, set to trigger alarm notifications, and automatically remediated in the future? (Choose two.)

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

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.S3 event may be lost in some cases, and could take up to minutes to arrive https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html
S3 event message does not contain information regarding permission
https://docs.aws.amazon.com/AmazonS3/latest/dev/notification-content-structure.html
B.Not sure where is the event comes from
C.We could take advice from trust advisor, but use a policy for trust advisor not going to help...
D.

**QUESTION 34**

A company is using an Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer. The web application requires user authorization and session tracking for dynamic content. The CloudFront distribution has a single cache behavior configured to forward the Authorization, Host, and User-Agent HTTP whitelist headers and a session cookie to the origin. All other cache behavior settings are set to their default value. A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings. The ACM certificate is also applied to the HTTPS listener for the Application Load Balancer. The CloudFront origin protocol policy is set to HTTPS only. Analysis of the cache statistics report shows that the miss rate for this distribution is very high. What can the Solutions Architect do to improve the cache hit rate for this distribution without causing the SSL/TLS handshake between CloudFront and the Application Load Balancer to fail?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Host header need to pass in as CloudFront and the origin are using the same certificate, which means the certificate's list of domain may not match the Origin Domain Name, and then hHost header is required
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/http-502-bad-gateway.html
B.Static content perform better without session cookie
C.HOST header is needed



**QUESTION 35**
An organization has a write-intensive mobile application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The application has scaled well, however, costs have increased exponentially because of higher than anticipated Lambda costs. The application's use is unpredictable, but there has been a steady 20% increase in utilization every month.
While monitoring the current Lambda functions, the Solutions Architect notices that the executiontime averages 4.5 minutes. Most of the wait time is the result of a high-latency network call to a 3-TB MySQL database server that is on-premises. A VPN is used to connect to the VPC, so the Lambda functions have been configured with a five-minute timeout. How can the Solutions Architect reduce the cost of the current architecture?

A. Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database.
Enable local caching in the mobile application to reduce the Lambda function invocation calls.Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.Offload the frequently accessed records from DynamoDB to Amazon ElastiCache.
B. Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database.
Cache the API Gateway results to Amazon CloudFront. Use Amazon EC2 Reserved Instances instead of Lambda.Enable Auto Scaling on EC2, and use Spot Instances during peak times.Enable DynamoDB Auto Scaling to manage target utilization.
C. Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.
Enable caching of the Amazon API Gateway results in Amazon CloudFront to reduce the number of Lambda function invocations.Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.Enable

DynamoDB Accelerator for frequently accessed records, and enable the DynamoDB Auto Scaling feature.

D. Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.
Enable API caching on API Gateway to reduce the number of Lambda function invocations.Continue to monitor the AWS Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.Enable Auto Scaling in DynamoDB.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will not help if the latency is from the on premise network (i.e. the on prem network itself is supper slow)
B.EC2 is more expensive, Direct Connect is not cheap as well
C.As the application is scaled well, we may not need DAX and cloudfront which cost more money. Moreover, if you use DAX, all request will go to DAX cluster first. You cannot just enable DAX for some records.

**QUESTION 36**
A company runs a video processing platform. Files are uploaded by users who connect to a web server, which stores them on an Amazon EFS share. This web server is running on a single Amazon EC2 instance. A different group of instances, running in an Auto Scaling group, scans the EFS share directory structure for new files to process and generates new videos (thumbnails, different resolution, compression, etc.) according to the instructions file, which is uploaded along with the video files. A different application running on a group of instances managed by an Auto Scaling group processes the video files and then deletes them from the EFS share. The results are stored in an S3 bucket. Links to the processed video files are emailed to the customer. The company has recently discovered that as they add more instances to the Auto Scaling Group, many files are processed twice, so image processing speed is not improved. The maximum size of these video files is 2GB. What should the Solutions Architect do to improve reliability and reduce the redundant processing of video files?

A. Modify the web application to upload the video files directly to Amazon S3. Use Amazon CloudWatch Events to trigger an AWS Lambda function every time a file is uploaded, and have this Lambda function put a message into an Amazon SQS queue. Modify the video processing application to read from SQS queue for new files and use the queue depth metric to scale instances in the video processing Auto Scaling group.
B. Set up a cron job on the web server instance to synchronize the contents of the EFS share into Amazon S3. Trigger an AWS Lambda function every time a file is uploaded to process the video file and store the results in Amazon S3. Using Amazon CloudWatch Events trigger an Amazon SES job to send an email to the customer containing the link to the processed file.
C. Rewrite the web application to run directly from Amazon S3 and use Amazon API Gateway to upload the video files to an S3 bucket. Use an S3 trigger to run an AWS Lambda function each time a file is uploaded to process and store new video files in a different bucket. Using CloudWatch Events, trigger an SES job to send an email to the customer containing the link to the processed file.
D. Rewrite the application to run from Amazon S3 and upload the video files to an S3 bucket.
Each time a new file is uploaded, trigger an AWS Lambda function to put a message in an SQS queue containing the link and the instructions. Modify the video processing application to read from the SQS queue and the S3 bucket. Use the queue depth metric to adjust the size of the Auto Scaling group for video processing instances.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Cloudwatch events do not support s3
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html
B.Cloudwatch events do not support s3
Lambda has concurrent limit
C.Lambda has 1000 concurrent execution. If every upload tried to trigger lambda to process video, this will not work
D.A queue is necessary as lambda execution has concurrent limit. Video processing can also take a long

time as the maximum size is 2GB. Lambda has execution limit of 900s and 1000 concurrent execution. 2GB memory is also a lot for lambda.
For option A, cloudwatch events is not supported for S3, you will need cloudtrail
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/EventTypes.html

**QUESTION 37**
A Solutions Architect must establish a patching plan for a large mixed fleet of Windows and Linux servers. The patching plan must be implemented securely, be audit ready, and comply with the company's business requirements. Which option will meet these requirements with MINIMAL effort?

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.AWS Config cannot monitor OS state
C.For OpsWorks the suggested way is to replace the old instance and during the setup security updates will be applied
https://docs.aws.amazon.com/opsworks/latest/userguide/workingsecurity-updates.html
D.OpsWork automatic patching only update the instance on setup
https://docs.aws.amazon.com/opsworks/latest/userguide/workingsecurity-updates.html

**QUESTION 38**
A Solutions Architect must design a highly available, stateless, REST service. The service will require multiple persistent storage layers for service object meta information and the delivery of content. Each request needs to be authenticated and securely processed. There is a requirement to keep costs as low as possible? How can these requirements be met?

A. Use AWS Fargate to host a container that runs a self-contained REST service. Set up an Amazon ECS service that is fronted by an Application Load Balancer (ALB). Use a custom authenticator to control access to the API. Store request meta information in Amazon DynamoDB with Auto Scaling and static content in a secured S3 bucket. Make secure signed requests for Amazon S3 objects and proxy the data through the REST service interface.
B. Use AWS Fargate to host a container that runs a self-contained REST service. Set up an ECS service that is fronted by a cross-zone ALB. Use an Amazon Cognito user pool to control access to the API. Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.
C. Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon Cognito user pool to control access to the API. Configure the methods to use AWS Lambda proxy integrations, and process each resource with a unique AWS Lambda function.
Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.
D. Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon API Gateway custom authorizer to control access to the API. Configure the methods to use AWS Lambda custom integrations, and process each resource with a unique Lambda function. Store request meta information in an Amazon ElastiCache Multi-AZ cluster and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**
A.One container is not HA, and custom authenticator is not a thing in ECS (it is in API Gateway). Alb support cognito or other IDP to authorise though, but this is vague in the answer. Also, you don't need to proxy the S3 content when using signed request.
B.One container is not HA, and Fargate container will not log API call logs like API gateway. ALB has access log though. This solution is overall much more expensive than C
D.ElastiCache is not persistent storage layer. Lambda custom integration is hard to use to process each request with a unique function, as you will need to define mappings for different endpoint using VTL.

**QUESTION 39**
A large company experienced a drastic increase in its monthly AWS spend. This is after Developers accidentally launched Amazon EC2 instances in unexpected regions. The company has established practices around least privileges for Developers and controls access to on-premises resources using Active Directory groups. The company now want to control costs by restricting the level of access that Developers have to the AWS Management Console without impacting their productivity. The company would also like to allow Developers to launch Amazon EC2 in only one region, without limiting access to other services in any region.
How can this company achieve these new security requirements while minimizing the administrative burden on the Operations team?

A. Set up SAML-based authentication tied to an IAM role that has an AdministrativeAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.
B. Create an IAM user for each Developer and add them to the developer IAM group that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that allows the Developers access to Amazon EC2 only in the required region.
C. Set up SAML-based authentication tied to an IAM role that has a PowerUserAccess managed policy and a customer managed policy that deny all the Developers access to any AWS services except AWS Service Catalog. Within AWS Service Catalog, create a product containing only the EC2 resources in the approved region.
D. Set up SAML-based authentication tied to an IAM role that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.



**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

A.AdministrativeAccess is not a managed policy. If we are talking about AdministratorAccess, this will give developer the power to change IAM policies and roles, which is not ideal and cannot stop them changing the deny policy to create EC2
B.IAM evaluation checks for at least allow if not deny is present. PowerUserAccess + allow in specific region will not stop access in other region
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-basics
C.This will limit access to other services，C不行的 题目说without limit other service

**QUESTION 40**
A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier. Company policy requires IT to durably store nightly backups f all its data in at least two locations: production and disaster recovery. The locations must be in different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location. All backup processes must be fully automated. What is the MOST cost-effective backup solution that will meet all requirements?

A. Back up all the data to a large Amazon EBS volume attached to the backup media server in the production region. Run automated scripts to snapshot these volumes nightly, and copy these snapshots to the disaster recovery region.

B. Back up all the data to Amazon S3 in the disaster recovery region. Use a lifecycle policy to move this data to Amazon Glacier in the production region immediately. Only the data is replicated; remove the data from the S3 bucket in the disaster recovery region.
C. Back up all the data to Amazon Glacier in the production region. Set up cross-region replication of this data to Amazon Glacier in the disaster recovery region. Set up a lifecycle policy to delete any data older than 60 days.
D. Back up all the data to Amazon S3 in the production region. Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.EBS is like 10 times more expensive than S3
B.Glacier retrieve can take up to hours (not S3 glacier though)
C.Glacier retrieve can take up to hours

**QUESTION 41**
A company has an existing on-premises three-tier web application. The Linux web servers serve content from a centralized file share on a NAS server because the content is refreshed several times a day from various sources. The existing infrastructure is not optimized and the company would like to move to AWS in order to gain the ability to scale resources up and down in response to load. On-premises and AWS resources are connected using AWS Direct Connect.
How can the company migrate the web infrastructure to AWS without delaying the content refresh process?

A. Create a cluster of web server Amazon EC2 instances behind a Classic Load Balancer on AWS. Share an Amazon EBS volume among all instances for the content. Schedule a periodic synchronization of this volume and the NAS server.
B. Create an on-premises file gateway using AWS Storage Gateway to replace the NAS server and replicate content to AWS. On the AWS side, mount the same Storage Gateway bucket to each web server Amazon EC2 instance to serve the content.
C. Expose an Amazon EFS share to on-premises users to serve as the NAS serve. Mount the same EFS share to the web server Amazon EC2 instances to serve the content.
D. Create web server Amazon EC2 instances on AWS in an Auto Scaling group. Configure a nightly process where the web server instances are updated from the NAS server.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.EBS volume can’t be shared across instances
B.Storge gateway is stored in S3, and you can’t mount a S3 bucket, officially.
C.This is good as EFS is a type of NAS and easy to support in this case
D.Up to 24 hour delay with the refresh process

**QUESTION 42**
A company has multiple AWS accounts hosting IT applications. An Amazon CloudWatch Logs agent is installed on all Amazon EC2 instances. The company wants to aggregate all security events in a centralized AWS account dedicated to log storage. Security Administrators need to perform near-real-time gathering and correlating of events across multiple AWS accounts.
Which solution satisfies these requirements?

A. Create a Log Audit IAM role in each application AWS account with permissions to view CloudWatch Logs, configure an AWS Lambda function to assume the Log Audit role, and perform an hourly export of CloudWatch Logs data to an Amazon S3 bucket in the logging AWS account.
B. Configure CloudWatch Logs streams in each application AWS account to forward events to CloudWatch Logs in the logging AWS account. In the logging AWS account, subscribe an Amazon Kinesis Data Firehose stream to Amazon CloudWatch Events, and use the stream to persist log data in Amazon S3.

C. Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to CloudWatch Logs streams in each application AWS account, configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams as its source, and persist the log data in an Amazon S3 bucket inside the logging AWS account.
D. Configure CloudWatch Logs agents to publish data to an Amazon Kinesis Data Firehose stream in the logging AWS account, use an AWS Lambda function to read messages from the stream and push messages to Data Firehose, and persist the data in Amazon S3.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Not near-real-time
B.CloudWatch event is not used to stream logs, and it cannot be used to stream logs
C.https://aws.amazon.com/blogs/architecture/central-logging-in-multi-account-environments/
D.CloudWatch agent cannot send logs directly to kinesis (maybe I am wrong)
Officially firehose cannot stream to lambda function, although you could use data transformation lambda to kind of do the trick, but this is bad practice.

**QUESTION 43**
A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified.
How can this be accomplished?

A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function. For changes to Lambda, create an 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.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Could use this for rollback trigger. But problem is API gateway also need to update to point to a different lambda version when update or rollback
B.Best practice
C.Need to update api gateway to point to other version
D.Not automatically. Also, API gateway endpoint with the same URL may not be possible

**QUESTION 44**
A company is running a .NET three-tier web application on AWS. The team currently uses XL storage optimized instances to store serve the website's image and video files on local instance storage. The company has encountered issues with data loss from replication and instance failures. The Solutions Architect has been asked to redesign this application to improve its reliability while keeping costs low.
Which solution will meet these requirements?

A. Set up a new Amazon EFS share, move all image and video files to this share, and then attach this new drive as a mount point to all existing servers. Create an Elastic Load Balancer with Auto Scaling general purpose instances. Enable Amazon CloudFront to the Elastic Load Balancer. Enable Cost Explorer and use AWS Trusted advisor checks to continue monitoring the environment for future savings.
B. Implement Auto Scaling with general purpose instance types and an Elastic Load Balancer.
Enable an Amazon CloudFront distribution to Amazon S3 and move images and video files to Amazon S3. Reserve general purpose instances to meet base performance requirements.
Use Cost Explorer and AWS Trusted Advisor checks to continue monitoring the environment for future savings.
C. Move the entire website to Amazon S3 using the S3 website hosting feature. Remove all the web servers and have Amazon S3 communicate directly with the application servers in Amazon VPC.
D. Use AWS Elastic Beanstalk to deploy the .NET application. Move all images and video files to Amazon EFS. Create an Amazon CloudFront distribution that points to the EFS share.
Reserve the m4.4xl instances needed to meet base performance requirements.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.S3 is a better option to keep cost low
C.S3 cannot communicate with other service… Other service can access S3. However, for this one if the application server don't have a nat, we will need VPC endpoint
D.Cloudfront cannot point to EFS directly

**QUESTION 45**
A company has developed a web application that runs on Amazon EC2 instances in one AWS Region. The company has taken on new business in other countries and must deploy its application into other to meet low-latency requirements for its users. The regions can be segregated, and an application running in one region does not need to communicate with instances in other regions.
How should the company's Solutions Architect automate the deployment of the application so that it can be MOST efficiently deployed into multiple regions?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
C.--region exists, but --regions is not a thing in aws CLI

**QUESTION 46**
A media company has a 30-TB repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.
The company has a high-speed AWS Direct Connect connection with AWS and would like to move the

MAM solution video content directly from its current file system. How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

A. Set up an AWS Storage Gateway, file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway.
Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.
B. Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway.
Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution.
C. Configure a video ingestion stream by using Amazon Kinesis Video Streams. Use the catalog of faces to build a collection in Amazon Rekognition. Stream the videos from the MAM solution into Kinesis Video Streams. Configure Amazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3.
D. Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required metadata, and push the metadata into the MAM solution while also copying the video files to an Amazon S3 bucket.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Tape will need to be restored somewhere before it can be accessed
C.I don't think you can config the video stream to save video in S3 directly (even though the video stream use S3 under the hood). You will need a consumer to so it. Also, this solution require manage a video stream, which feels a lot of overhead as we don't really need real time processing here.
https://github.com/awslabs/amazon-kinesis-video-streams-producer-sdk-java/issues/22
D.EBS maximum size is 16TB



**QUESTION 47**
A company is planning the migration of several lab environments used for software testing. An assortment of custom tooling is used to manage the test runs for each lab. The labs use immutable infrastructure for the software test runs, and the results are stored in a highly available SQL database cluster. Although completely rewriting the custom tooling is out of scope for the migration project, the company would like to optimize workloads during the migration.
Which application migration strategy meets this requirement?

A. Re-host
B. Re-platform
C. Re-factor/re-architect
D. Retire

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 48**
A company is implementing a multi-account strategy; however, the Management team has expressed concerns that services like DNS may become overly complex. The company needs a solution that allows private DNS to be shared among virtual private clouds (VPCs) in different accounts. The company will have approximately 50 accounts in total. What solution would create the LEAST complex DNS architecture and

ensure that each VPC can resolve all AWS resources?

A. Create a shared services VPC in a central account, and create a VPC peering connection from the shared services VPC to each of the VPCs in the other accounts. Within Amazon Route 53, create a privately hosted zone in the shared services VPC and resource record sets for the domain and subdomains. Programmatically associate other VPCs with the hosted zone.
B. Create a VPC peering connection among the VPCs in all accounts. Set the VPC attributes enableDnsHostnames and enableDnsSupport to "true" for each VPC. Create an Amazon Route 53 private zone for each VPC. Create resource record sets for the domain and subdomains. Programmatically associate the hosted zones in each VPC with the other VPCs.
C. Create a shared services VPC in a central account. Create a VPC peering connection from the VPCs in other accounts to the shared services VPC. Create an Amazon Route 53 privately hosted zone in the shared services VPC with resource record sets for the domain and subdomains. Allow UDP and TCP port 53 over the VPC peering connections.
D. Set the VPC attributes enableDnsHostnames and enableDnsSupport to "false" in every VPC. Create an AWS Direct Connect connection with a private virtual interface. Allow UDP and TCP port 53 over the virtual interface. Use the on-premises DNS servers to resolve the IP addresses in each VPC on AWS.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.One thing need to keep in mind: The association need to be done programmatically as the private hosted zone is not in the same account as the VPC we try to associate to.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs-different-accounts.html
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs.html
B.enableDnsHostnames: Used to determine if resource within VPC with public IP get a public hostname
enableDnsSupport: Used to determine if AWS DNS is supported in the VPC
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html
This will actually work, but really not necessary as you will have 50 hosted zone to manage and 50*49 VPC peering need to config...However, as each VPC will have different Route 53 zone, this is not sharing a DNS
C.You don't really need to allow port 53 as VPC peering doesn't block anything, this is NACL's job. However, the Route 53 Hosted Zone need to be associated to VPCs to work
D.This can be ruled out immediately as direct connection is used for On-Prem to aws connect

**QUESTION 49**
A company has asked a Solutions Architect to design a secure content management solution that can be accessed by API calls by external customer applications. The company requires that a customer administrator must be able to submit an API call and roll back changes to existing files sent to the content management solution, as needed.

What is the MOST secure deployment design that meets all solution requirements?

A. Use Amazon S3 for object storage with versioning and bucket access logging enabled, and an IAM role and access policy for each customer application. Encrypt objects using SSE-KMS.
Develop the content management application 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.

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will work. With HTTPS we could even do encryption in transit. You can specify key on your S3 request header.
https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPUT.html
B.WorkDocs is really not designed for this...
C.You could specify encryption key for EFS, but this should be done with KMS policies. EFS access policies is used to control things like management access, not file access
https://docs.aws.amazon.com/efs/latest/ug/efs-api-permissions-ref.html
D.Deliver keys to client is not very secure.

**QUESTION 50**
A company has released a new version of a website to target an audience in Asia and South America. The website's media assets are hosted on Amazon S3 and have an Amazon CloudFront distribution to improve end-user performance. However, users are having a poor login experience the authentication service is only available in the us-east-1 AWS Region. How can the Solutions Architect improve the login experience and maintain high security and performance with minimal management overhead?

A. Replicate the setup in each new geography and use Amazon Route S3 geo-based routing to route traffic to the AWS Region closest to the users.
B. Use an Amazon Route S3 weighted routing policy to route traffic to the CloudFront distribution. Use CloudFront cached HTTP methods to improve the user login experience.
C. Use Amazon Lambda@Edge attached to the CloudFront viewer request trigger to authenticate and authorize users by maintaining a secure cookie token with a session expiry to improve the user experience in multiple geographies.
D. Replicate the setup in each geography and use Network Load Balancers to route traffic to the authentication service running in the closest region to users.



**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Too much overhead...
B.Login cannot be cached
C.https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-generating-http-responses-in-requests.html
D.Overhead!! And network load balancer cannot do this

**QUESTION 51**
A company has a standard three-tier architecture using two Availability Zones. During the company's off season, users report that the website is not working. The Solutions Architect finds that no changes have been made to the environment recently, the website is reachable, and it is possible to log in. However, when the Solutions Architect selects the "find a store near you" function, the maps provided on the site by a third-party RESTful API call do not work about 50% of the time after refreshing the page. The outbound API calls are made through Amazon EC2 NAT instances.
What is the MOST likely reason for this failure and how can it be mitigated in the future?

A. The network ACL for one subnet is blocking outbound web traffic. Open the network ACL and prevent administration from making future changes through IAM.
B. The fault is in the third-party environment. Contact the third party that provides the maps and request a fix that will provide better uptime.
C. One NAT instance has become overloaded. Replace both EC2 NAT instances with a larger-sized instance and make sure to account for growth when making the new instance size.
D. One of the NAT instances failed. Recommend replacing the EC2 NAT instances with a NAT gateway.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Cannot be this as 50% of the call succeed
C.Could work but not really a good solution for scalability

**QUESTION 52**
A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.
Which would enable the collection of this data MOST cost effectively?

A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.
B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.
C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.
D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.CloudWatch agent is used to send log item and do not monitor network traffic
C.Agentless discovery cannot get process information
https://aws.amazon.com/application-discovery/faqs/#

**QUESTION 53**
A company will several AWS accounts is using AWS Organizations and service control policies (SCPs). An Administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:

```
{
"Version": "2012-10-27"
"Statement": [
{
"Side": "AllowsAllActions",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
},
{
"Side": "DenyCloudTrail",
"Effect": "Deny",
"Action": "CloudTrail:*",
"Resource": "*"
}
]
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets.
How should the Administrator address this problem?

A. Add s3:CreateBucket with "Allow" effect to the SCP.
B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
C. Instruct the Developers to add Amazon S3 permissions to their IAM entities.
D. Remove the SCP from account 1111-1111-1111.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Explicit deny will overwrite any allow
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html
B.Will still stop the action
C.IAM cannot overwrite SCP, both of them need to allow the action, but the policy did not deny create s3 bucket permission
D.Will work, probably not the best choice
There should be a SCP written somewhere, but B, C and D doesn't look correct at all.
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

**QUESTION 54**
A company that provides wireless services needs a solution to store and analyze log files about user activities. Currently, log files are delivered daily to Amazon Linux on Amazon EC2 instance. A batch script is run once a day to aggregate data used for analysis by a third-party tool. The data pushed to the thirdparty tool is used to generate a visualization for end users. The batch script is cumbersome to maintain, and it takes several hours to deliver the ever-increasing data volumes to the third-party tool. The company wants to lower costs, and is open to considering a new tool that minimizes development effort and lowers administrative overhead. The company wants to build a more agile solution that can store and perform the analysis in near-real time, with minimal overhead. The solution needs to be cost effective and scalable to meet the company's end-user base growth.
Which solution meets the company's requirements?

A. Develop a Python script to failure the data from Amazon EC2 in real time and store the data in Amazon S3. Use a copy command to copy data from Amazon S3 to Amazon Redshift.
Connect a business intelligence tool running on Amazon EC2 to Amazon Redshift and create the visualizations.
B. Use an Amazon Kinesis agent running on an EC2 instance in an Auto Scaling group to collect and send the data to an Amazon Kinesis Data Forehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data directly to Amazon ES. Use Kibana to visualize the data.
C. Use an in-memory caching application running on an Amazon EBS-optimized EC2 instance to capture the log data in near real-time. Install an Amazon ES cluster on the same EC2 instance to store the log files as they are delivered to Amazon EC2 in near real-time.
Install a Kibana plugin to create the visualizations.
D. Use an Amazon Kinesis agent running on an EC2 instance to collect and send the data to an Amazon Kinesis Data Firehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data to Amazon S3. Use an AWS Lambda function to deliver the data from Amazon S3 to Amazon ES. Use Kibana to visualize the data.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
72
A.Python script will be become the hard part to maintain
C.Too many EC2s, very expensive
D.Firehose can deliver to ES direcly
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-aws-integrations.html

**QUESTION 55**
A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability. Which service will meet the requirements for storing the session information in the MOST costeffective way?

A. Amazon ElastiCache with the Memcached engine
B. Amazon S3
C. Amazon RDS MySQL
D. Amazon ElastiCache with the Redis engine

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Memcached is not really HA (no replication)
https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug/SelectEngine.html

**QUESTION 56**
A company has an Amazon EC2 deployment that has the following architecture:
* An application tier that contains 8 m4.xlarge instances
* A Classic Load Balancer
* Amazon S3 as a persistent data store
After one of the EC2 instances fails, users report very slow processing of their requests. A Solutions Architect must recommend design changes to maximize system reliability. The solution must minimize costs.
What should the Solution Architect recommend?

A. Migrate the existing EC2 instances to a serverless deployment using AWS Lambda functions
B. Change the Classic Load Balancer to an Application Load Balancer
C. Replace the application tier with m4.large instances in an Auto Scaling group
D. Replace the application tier with 4 m4.2xlarge instances

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 57**
An on-premises application will be migrated to the cloud. The application consists of a single Elasticsearch virtual machine with data source feeds from local systems that will not be migrated, and a Java web application on Apache Tomcat running on three virtual machines. The Elasticsearch server currently uses 1 TB of storage out of 16 TB available storage, and the web application is updated every 4 months. Multiple users access the web application from the Internet. There is a 10Gbit AWS Direct Connect connection established, and the application can be migrated over a schedules 48-hour change window. Which strategy will have the LEAST impact on the Operations staff after the migration?

A. Create an Elasticsearch server on Amazon EC2 right-sized with 2 TB of Amazon EBS and a public AWS Elastic Beanstalk environment for the web application. Pause the data sources, export the Elasticsearch index from on premises, and import into the EC2 Elasticsearch server.
Move data source feeds to the new Elasticsearch server and move users to the web application.
B. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Use AWS DMS to replicate Elasticsearch data. When replication has finished, move data source feeds to the new Amazon ES cluster endpoint and move users to the new web application.
C. Use the AWS SMS to replicate the virtual machines into AWS. When the migration is complete, pause the data source feeds and start the migrated Elasticsearch and web application instances. Place the web application instances behind a public Elastic Load Balancer. Move the data source feeds to the new Elasticsearch server and move users to the new web Application Load Balancer.
D. Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Pause the data source feeds, export the Elasticsearch index from on premises, and import into the Amazon ES cluster. Move the data source feeds to the new Amazon ES cluster endpoint and move users to the new web application.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.ES cannot be the source of DMS

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.html
D.By import and export, I think it means snapshot and restore, otherwise there is no export or import of an index in ElasticSearch. If this is the case, this is the best answer, otherwise C will be the only viable solution….

**QUESTION 58**
A company's application is increasingly popular and experiencing latency because of high volume reads on the database server.
The service has the following properties:
* A highly available REST API hosted in one region using Application Load Balancer (ALB) with auto scaling.
* A MySQL database hosted on an Amazon EC2 instance in a single Availability Zone.
* The company wants to reduce latency, increase in-region database read performance, and have multi-region disaster recovery capabilities that can perform a live recovery automatically without any data or performance loss (HA/DR). Which deployment strategy will meet these requirements?

A. Use AWS CloudFormation StackSets to deploy the API layer in two regions. Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region and a read replica in a different region than the source database cluster. Use Amazon Route 53 health checks to trigger a DNS failover to the standby region if the health checks to the primary load balancer fail. In the event of Route 53 failover, promote the cross-region database replica to be the master and build out new read replicas in the standby region.
B. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. In the event of failure, use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.
C. Use AWS CloudFormation StackSets to deploy the API layer in two regions. Add the database to an Auto Scaling group. Add a read replica to the database in the second region.
Use Amazon Route 53 health checks in the primary region fail. Promote the cross-region database replica to be the master and build out new read replicas in the standby region.
D. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. Use Amazon Route 53 health checks on the ALB to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Aurora cluster is multi AZ by default, this is the best option
B.Cannot live failover DB
C.Share data volume across EC2 will be painful
D.Same as B

**QUESTION 59**
A company runs a three-tier application in AWS. Users report that the application performance can vary greatly depending on the time of day and functionality being accessed.
The application includes the following components:
* Eight t2.large front-end web servers that serve static content and proxy dynamic content from the application tier.
* Four t2.large application servers.
* One db.m4.large Amazon RDS MySQL Multi-AZ DB instance. Operations has determined that the web and application tiers are network constrained. Which of the following should cost effective improve application performance? (Choose two.)

A. Replace web and app tiers with t2.xlarge instances
B. Use AWS Auto Scaling and m4.large instances for the web and application tiers
C. Convert the MySQL RDS instance to a self-managed MySQL cluster on Amazon EC2

D. Create an Amazon CloudFront distribution to cache content
E. Increase the size of the Amazon RDS instance to db.m4.xlarge

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
As the constraint is network, t2.xlarge has the same network performance as m4.large, but more expensive
https://aws.amazon.com/ec2/pricing/on-demand/
https://aws.amazon.com/ec2/instance-types/

**QUESTION 60**
An online retailer needs to regularly process large product catalogs, which are handled in batches. These are sent out to be processed by people using the Amazon Mechanical Turk service, but the retailer has asked its Solutions Architect to design a workflow orchestration system that allows it to handle multiple concurrent Mechanical Turk operations, deal with the result assessment process, and reprocess failures. Which of the following options gives the retailer the ability to interrogate the state of every workflow with the LEAST amount of implementation effort?

A. Trigger Amazon CloudWatch alarms based upon message visibility in multiple Amazon SQS queues (one queue per workflow stage) and send messages via Amazon SNS to trigger AWS Lambda functions to process the next step. Use Amazon ES and Kibana to visualize Lambda processing logs to see the workflow states.
B. Hold workflow information in an Amazon RDS instance with AWS Lambda functions polling RDS for status changes. Worker Lambda functions then process the next workflow steps. Amazon QuickSight will visualize workflow states directly out of Amazon RDS.
C. Build the workflow in AWS Step Functions, using it to orchestrate multiple concurrent workflows. The status of each workflow can be visualized in the AWS Management Console, and historical data can be written to Amazon S3 and visualized using Amazon QuickSight.
D. Use Amazon SWF to create a workflow that handles a single batch of catalog records with multiple worker tasks to extract the data, transform it, and send it through Mechanical Turk.
Use Amazon ES and Kibana to visualize AWS Lambda processing logs to see the workflow states.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
C.Step Function may not work really well with human intervention, and I don't think historical data can be easily pipe to S3
D.Workflow is best to be dealt with by SWF or Step Function, so A and B are excluded.
As we are using Mechanical Turk HITs, manual intervention will be needed (i.e. accessed for successful result). There is also a similar use case with SWF in https://aws.amazon.com/swf/faqs/

**QUESTION 61**
An organization has two Amazon EC2 instances:
* The first is running an ordering application and an inventory application.
* The second is running a queuing system.
During certain times of the year, several thousand orders are placed per second. Some orders were lost when the queuing system was down. Also, the organization's inventory application has the incorrect quantity of products because some orders were processed twice.
What should be done to ensure that the applications can handle the increasing number of orders?

A. Put the ordering and inventory applications into their own AWS Lambda functions. Have the ordering application write the messages into an Amazon SQS FIFO queue.
B. Put the ordering and inventory applications into their own Amazon ECS containers and create an Auto Scaling group for each application. Then, deploy the message queuing server in multiple Availability Zones.
C. Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each application. Use Amazon SQS standard queues for the incoming orders, and implement idempotency in the inventory application.

D. Put the ordering and inventory applications into their own Amazon EC2 instances. Write the incoming orders to an Amazon Kinesis data stream Configure AWS Lambda to poll the stream and update the inventory application.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This looks like a good solution but it actually won't work as Lambda has a concurrent limit for 1000 and we need to process thousands of orders per second. (although we could contact AWS to increase the limit, but doesn't feel like a good answer for the exam).
B.Distributed queueing system will probably have duplicate messages at some point. Also, auto scale group is not a thing in ECS (it is for EC2 that backed the ECS though)
D.Kinesis stream has no message level ack/fail, still will have duplicate or unprocessed items

**QUESTION 62**
A company is migrating its on-premises build artifact server to an AWS solution. The current system consists of an Apache HTTP server that serves artifacts to clients on the local network, restricted by the perimeter firewall. The artifact consumers are largely build automation scripts that download artifacts via anonymous HTTP, which the company will be unable to modify within its migration timetable.
The company decides to move the solution to Amazon S3 static website hosting. The artifact consumers will be migrated to Amazon EC2 instances located within both public and private subnets in a virtual private cloud (VPC).
Which solution will permit the artifact consumers to download artifacts without modifying the existing automation scripts?

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will go through the public internet, apparently not the best option
C.Instances in private subnet cannot access the bucket
D.For S3 with VPC endpoint, you cannot use sourceip with VPC CIDR block
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html

**QUESTION 63**
A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs for requests and data transfers from Amazon S3.
Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers?

A. Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Have the organizations assume and use that read role when accessing the data.

B. Ensure that all organizations in the partnership have AWS accounts. Create a bucket policy on the bucket that owns the data. The policy should allow the accounts in the partnership read access to the bucket. Enable Requester Pays on the bucket. Have the organizations use their AWS credentials when accessing the data.
C. Ensure that all organizations in the partnership have AWS accounts. Configure buckets in each of the accounts with a bucket policy that allows the institute that owns the data the ability to write to the bucket. Periodically sync the data from the institute's account to the other organizations. Have the organizations use their AWS credentials when accessing the data using their accounts.
D. Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Enable Requester Pays on the bucket. Have the organizations assume and use that read role when accessing the data.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.The organization that owns the data will pay for everything
C.This will cause double charge: write and read
D.Account that owns the assumed role will be charged with Requester Pays..
https://docs.aws.amazon.com/AmazonS3/latest/dev/RequesterPaysBuckets.html

https://amazonaws-china.com/cn/premiumsupport/knowledge-center/s3-cross-account-a ccess-denied/

**QUESTION 64**
A company currently uses a single 1 Gbps AWS Direct Connect connection to establish connectivity between an AWS Region and its data center. The company has five Amazon VPCs, all of which are connected to the data center using the same Direct Connect connection. The Network team is worried about the single point of failure and is interested in improving the redundancy of the connections to AWS while keeping costs to a minimum. Which solution would improve the redundancy of the connection to AWS while meeting the cost requirements?

A. Provision another 1 Gbps Direct Connect connection and create new VIFs to each of the VPCs. Configure the VIFs in a load balancing fashion using BGP.
B. Set up VPN tunnels from the data center to each VPC. Terminate each VPN tunnel at the virtual private gateway (VGW) of the respective VPC and set up BGP for route management.
C. Set up a new point-to-point Multiprotocol Label Switching (MPLS) connection to the AWS Region that's being used. Configure BGP to use this new circuit as passive, so that no traffic flows through this unless the AWS Direct Connect fails.
D. Create a public VIF on the Direct Connect connection and set up a VPN tunnel which will terminate on the virtual private gateway (VGW) of the respective VPC using the public VIF.
Use BGP to handle the failover to the VPN connection.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.VIF is not VGW, it is associated to direct connect
https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/
C.MPLS still go through direct connect
https://aws.amazon.com/answers/networking/aws-network-connectivity-over-mpls/
D.You don’t need a public VIF unless you need to connect to AWS public service, and you don’t need public VIF for VPN connection

**QUESTION 65**
A company currently uses Amazon EBS and Amazon RDS for storage purposes. The company intends to use a pilot light approach for disaster recovery in a different AWS Region. The company has an RTO of 6 hours and an RPO of 24 hours. Which solution would achieve the requirements with MINIMAL cost?

A. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.
B. Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group configured in the same way as in the primary region.
C. Use Amazon ECS to handle long-running tasks to create daily EBS and RDS snapshots, and copy to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region
D. Use EBS and RDS cross-region snapshot copy capability to create snapshots in the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Lambda should not be used for snapshot
B.'EC2 configure the same way' will be Multi-Site
D.Use built-in cross region copy will be the best solution, but EBS cannot take snapshot automatically, you will need AWS data lifecycle

**QUESTION 66**
A company needs to cost-effectively persist small data records (up to 1 KiB) for up to 30 days. The data is read rarely. When reading the data, a 5-minute delay is acceptable. Which of the following solutions achieve this goal? (Choose two.)

A. Use Amazon S3 to collect multiple records in one S3 object. Use a lifecycle configuration to move data to Amazon Glacier immediately after write. Use expedited retrievals when reading the data.
B. Write the records to Amazon Kinesis Data Firehose and configure Kinesis Data Firehose to deliver the data to Amazon S3 after 5 minutes. Set an expiration action at 30 days on the S3 bucket.
C. Use an AWS Lambda function invoked via Amazon API Gateway to collect data for 5 minutes. Write data to Amazon S3 just before the Lambda execution stops.
D. Write the records to Amazon DynamoDB configured with a Time To Live (TTL) of 30 days. Read data using the GetItem or BatchGetItem call.
E. Write the records to an Amazon ElastiCache for Redis. Configure the Redis append-only file (AOF) persistence logs to write to Amazon S3. Recover from the log if the ElastiCache instance has failed.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Glacier retrieval can be up to 1-5 mins, and Glacier has a minimum size charge of 40KB, but the minimum storage time charge is 90 days, even though it is still much cheaper than standard S3
https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html
https://aws.amazon.com/s3/storage-classes/
B.I think it means buffer interval for firehose here. The cost is tricky as each record round up to the nearest 5 KB for charging, as the record is all 1 KB, we could pay 5 times more in this case for firehose.
https://docs.aws.amazon.com/firehose/latest/dev/basic-deliver.html#frequency
C.This is not a really robust solution as we have long running lambda, which is not what lambda intend to do. It will be quite costly. API gateway will also timeout after 30s.
D.AOF write to s3 is not supported
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/RedisAOF.html

**QUESTION 67**
A Development team is deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS Lambda, and Amazon DynamoDB resources. A Solutions Architect has been tasked with automating the future deployments of these serverless APIs.

How can this be accomplished?

A. Use AWS CloudFormation with a Lambda-backed custom resource to provision API Gateway. Use the AWS::DynamoDB::Table and AWS::Lambda::Function resources to create the Amazon DynamoDB table and Lambda functions. Write a script to automate the deployment of the CloudFormation template.
B. Use the AWS Serverless Application Model to define the resources. Upload a YAML template and application files to the code repository. Use AWS CodePipeline to connect to the code repository and to create an action to build using AWS CodeBuild. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution.
C. Use AWS CloudFormation to define the serverless application. Implement versioning on the Lambda functions and create aliases to point to the versions. When deploying, configure weights to implement shifting traffic to the newest version, and gradually update the weights as traffic moves over.
D. Commit the application code to the AWS CodeCommit code repository. Use AWS CodePipeline and connect to the CodeCommit code repository. Use AWS CodeBuild to build and deploy the Lambda functions using AWS CodeDeploy. Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.API Gateway cloudformation is supported, custom resource is not necessary
B.SAM deploy is just an alias of cloudformation deploy
https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/sam-cli-command-reference-sam-deploy.html
Codebuild can put artifacts in S3 for later lambda deployment.
https://docs.aws.amazon.com/codebuild/latest/APIReference/API_ProjectArtifacts.html
C.We will need either codedeploy or step function to achieve traffic shift, this answer is too vague
D.API Gateway and lambda resource is not deployed

**QUESTION 68**
The company Security team queries that all data uploaded into an Amazon S3 bucket must be encrypted. The encryption keys must be highly available and the company must be able to control access on a per-user basis, with different users having access to different encryption keys.
Which of the following architectures will meet these requirements? (Choose two.)

A. Use Amazon S3 server-side encryption with Amazon S3-managed keys. Allow Amazon S3 to generate an AWS/S3 master key, and use IAM to control access to the data keys that are generated.
B. Use Amazon S3 server-side encryption with AWS KMS-managed keys, create multiple customer master keys, and use key policies to control access to them.
C. Use Amazon S3 server-side encryption with customer-managed keys, and use AWS CloudHSM to manage the keys. Use CloudHSM client software to control access to the keys that are generated.
D. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use the Cloud HSM client software to control access to the keys that are generated.
E. Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use IAM to control access to the keys that are generated in CloudHSM.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.S3 generated keys cannot be managed
C.One HSM is not HA
E.CloudHSM cannot communicate with any aws services

**QUESTION 69**
A company runs a public-facing application that uses a Java-based web service via a RESTful API. It is hosted on Apache Tomcat on a single server in a data center that runs consistently at 30% CPU utilization.

Use of the API is expected to increase by 10 times with a new product launch. The business wants to migrate the application to AWS with no disruption, and needs it to scale to meet demand. The company has already decided to use Amazon Route 53 and CNAME records to redirect traffic. How can these requirements be met with the LEAST amount of effort?

A. Use AWS Elastic Beanstalk to deploy the Java web service and enable Auto Scaling. Then switch the application to use the new web service.
B. Lift and shift the Apache server to the cloud using AWS SMS. Then switch the application to direct web service traffic to the new instance.
C. Create a Docker image and migrate the image to Amazon ECS. Then change the application code to direct web service queries to the ECS container.
D. Modify the application to call the web service via Amazon API Gateway. Then create a new AWS Lambda Java function to run the Java web service code. After testing, change API Gateway to use the Lambda function.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This is best as replatform makes sense
B.Re-host may not improve much
C.Will need load balancer and auto scaling..
D.A lot of work as this is re-architect

**QUESTION 70**
A company is using AWS for production and development workloads. Each business unit has its own AWS account for production, and a separate AWS account to develop and deploy its applications. The Information Security department has introduced new security policies that limit access for terminating certain Amazon ECs instances in all accounts to a small group of individuals from the Security team. How can the Solutions Architect meet these requirements?

A. Create a new IAM policy that allows access to those EC2 instances only for the Security team. Apply this policy to the AWS Organizations master account.
B. Create a new tag-based IAM policy that allows access to these EC2 instances only for the Security team. Tag the instances appropriately, and apply this policy in each account.
C. Create an organizational unit under AWS Organizations. Move all the accounts into this organizational unit and use SCP to apply a whitelist policy to allow access to these EC2 instances for the Security team only.
D. Set up SAML federation for all accounts in AWS. Configure SAML so that it checks for the service API call before authenticating the user. Block SAML from authenticating API calls if anyone other than the Security team accesses these instances.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.IAM policy will not be applied to sub account
C.SCP is not for granular access control. SCP will not actually grant permission as well
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html
D.This just won't work as SAML will work like token base service and do not rely on the API calls

**QUESTION 71**
A company is moving a business-critical, multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A Solutions Architect must re-architect the application to ensure that it can meet or exceed the SLA. The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application.
Which of the following will meet the availability requirements with little change to the application while

improving user experience and minimizing costs?

A. Migrate the database to a PostgreSQL database in Amazon EC2. Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Allocate an Amazon WorkSpaces WorkSpace for each end user to improve the user experience.
B. Migrate the database to an Amazon RDS Aurora PostgreSQL configuration. Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer. Use Amazon AppStream 2.0 to improve the user experience.
C. Migrate the database to an Amazon RDS PostgreSQL Multi-AZ configuration. Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balancer. Use Amazon ElastiCache to improve the user experience.
D. Migrate the database to an Amazon Redshift cluster with at least two nodes. Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Use Amazon CloudFront to improve the user experience.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Database in EC2 may not be the best option
C.Using ElastiCache will require some changes to the application
D.Redshift not design for this. Even though it may work, the price is high.

**QUESTION 72**
A company has a 24 TB MySQL database in its on-premises data center that grows at the rate of 10 GB per day. The data center is connected to the company's AWS infrastructure with a 50 Mbps VPN connection.
The company is migrating the application and workload to AWS. The application code is already installed and tested on Amazon EC2. The company now needs to migrate the database and wants to go live on AWS within 3 weeks.
Which of the following approaches meets the schedule with LEAST downtime?

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

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 73**
A company is designing a new highly available web application on AWS. The application requires consistent and reliable connectivity from the application servers in AWS to a backend REST API hosted in the company's on-premises environment. The backend connection between AWS and on-premises will be routed over an AWS Direct Connect connection through a private virtual interface. Amazon Route 53 will be used to manage private DNS records for the application to resolve the IP address on the backend REST API.
Which design would provide a reliable 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.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 74**
A company has a data center that must be migrated to AWS as quickly as possible. The data center has a 500 Mbps AWS Direct Connect link and a separate, fully available 1 Gbps ISP connection. A Solutions Architect must transfer 20 TB of data from the data center to an Amazon S3 bucket.
What is the FASTEST way transfer the data?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 75**
A bank is designing an online customer service portal where customers can chat with customer service agents. The portal is required to maintain a 15-minute RPO or RTO in case of a regional disaster. Banking regulations require that all customer service chat transcripts must be preserved on durable storage for at least 7 years, chat conversations must be encrypted in-flight, and transcripts must be encrypted at rest. The Data Lost Prevention team requires that data at rest must be encrypted using a key that the team controls, rotates, and revokes.
Which design meets these requirements?

A. The chat application logs each chat message into Amazon CloudWatch Logs. A scheduled AWS Lambda function invokes a CloudWatch Logs. CreateExportTask every 5 minutes to export chat transcripts to Amazon S3. The S3 bucket is configured for cross-region replication to the backup region.

Separate AWS KMS keys are specified for the CloudWatch Logs group and the S3 bucket.

B. The chat application logs each chat message into two different Amazon CloudWatch Logs groups in two different regions, with the same AWS KMS key applied. Both CloudWatch Logs groups are configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy with a KMS key specified.

C. The chat application logs each chat message into Amazon CloudWatch Logs. A subscription filter on the CloudWatch Logs group feeds into an Amazon Kinesis Data Firehose which streams the chat messages into an Amazon S3 bucket in the backup region.
Separate AWS KMS keys are specified for the CloudWatch Logs group and the Kinesis Data Firehose.

D. The chat application logs each chat message into Amazon CloudWatch Logs. The CloudWatch Logs group is configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy. Glacier cross-region replication mirrors chat archives to the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Amazon Glacier vault.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.By Default, cross-region replication will not replicate SSE-KMS objects, this need to be enabled explicitly with relevant info (KMS keys access)
Moreover, cloudwatch export to SSE-KMS encrypted S3 is not supported
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/S3Export.html
B.Before S3 Glacier, you couldn't export directly to glacier from cloudwatch
Moreover, cloudwatch export to SSE-KMS encrypted S3 is not supported, I will apply the same to glacier
And you can not use KMS CMK across region
https://forums.aws.amazon.com/thread.jspa?threadID=287340
C.Kinesis Firehose can encrypt S3 at rest https://docs.aws.amazon.com/firehose/latest/dev/create-configure.html
D.Before S3 Glacier, you couldn't export directly to glacier from cloudwatch
Moreover, cloudwatch export to SSE-KMS encrypted S3 is not supported
IF we are talking about S3 glacier, as cloudwatch only available in one region, and glacier may take hours to retrieve data, 15 mins RTO cannot be done

**QUESTION 76**
A company currently runs a secure application on Amazon EC2 that takes files from onpremises locations through AWS Direct Connect, processes them, and uploads them to a single Amazon S3 bucket. The application uses HTTPS for encryption in transit to Amazon S3, and S3 serverside encryption to encrypt at rest.
Which of the following changes should the Solutions Architect recommend to make this solution more secure without impeding application's performance?

A. Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the NAT gateway's Elastic IP address only.

B. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required Amazon S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC's source IP range only.

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

D. Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC endpoint only.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Request go through the internet will be even less secure
B.You cannot use sourceIp in s3 bucket policy for VPC endpoint
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html
C.Same as A

D.aws:sourceVpce

**QUESTION 77**
As a part of building large applications in the AWS Cloud, the Solutions Architect is required to implement the perimeter security protection. Applications running on AWS 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 must design a solution to protect all of the listed web front ends and provide the following security capabilities:
* DDoS protection
* SQL injection protection
* IP address whitelist/blacklist
* HTTP flood protection
* Bad bot scraper protection
How should the Solutions Architect design the solution?

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.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
CloudFront and AWS Shield Advanced is good with DDoS while WAF will support blocking IPs, SQL injection attacks and Bad Bots.



**QUESTION 78**
A company has more than 100 AWS accounts, with one VPC per account, that need outbound HTTPS connectivity to the internet. The current design contains one NAT gateway per Availability Zone (AZ) in each VPC. To reduce costs and obtain information about outbound traffic, management has asked for a new architecture for internet access. Which solution will meet the current needs, and continue to grow as new accounts are provisioned, while reducing costs?

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.https://aws.amazon.com/answers/networking/aws-single-region-multi-vpc-connectivity/
B.Route traffic back to on-prem for internet access is a bad practice
C.You cannot route traffic to NAT gateway through a VPC peering
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

D.PrivateLink cannot be used to route internet traffic
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html

**QUESTION 79**
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 additional steps will address all of other identical attack types while providing high availability and minimizing 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.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.We don’t need SSH anymore as system manager can run command and do patches.
C.We don’t need SSH anymore as system manager can run command and do patches. Also mysql with ec2 is not that good
D.RDS Single-AZ is not HA

**QUESTION 80**
A company has a High Performance Computing (HPC) cluster in its on-premises data center which runs thousands of jobs in parallel for one week every month, processing petabytes of images. The images are stored on a network file server, which is replicated to a disaster recovery site. The onpremises data center has reached capacity and has started to spread the jobs out over the course of month in order to better utilize the cluster, causing a delay in the job completion.
The company has asked its Solutions Architect to design a cost-effective solution on AWS to scale beyond the current capacity of 5,000 cores and 10 petabytes of data. The solution must require the least amount of management overhead and maintain the current level of durability.
Which solution will meet the company's requirements?

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.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.It is hard to do and maintain as EBS has maximum size limit of 16TB and cannot be mounted to multiple instances
B.DynamoDb is not the best places to store job item because of its nature of eventual consistency
D.S3 could be the better storage option here

**QUESTION 81**
A large company has many business units. Each business unit has multiple AWS accounts for different purposes. The CIO of the company sees that each business unit has data that would be useful to share with other parts of the company in total, there are about 10 PB of data that needs to be shared with users in 1,000 AWS accounts. The data is proprietary, so some of it should only be available to users with specific job types. Some of the data is used for throughput of intensive workloads, such as simulations. The number of accounts changes frequently because of new initiatives, acquisitions, and divestitures. A Solutions Architect has been asked to design a system that will allow for sharing data for use in AWS with all of the employees in the company. Which approach will allow for secure data sharing in scalable way?

A. Store the data in a single Amazon S3 bucket. Create an IAM role for every combination of job type and business unit that allows to appropriate read/write access based on object prefixes in the S3 bucket. The roles should have trust policies that allow the business unit's AWS accounts to assume their roles. Use IAM in each business unit's AWS account to prevent them from assuming roles for a different job type. Users get credentials to access the data by using AssumeRole from their business unit's AWS account. Users can then use those credentials with an S3 client.

B. Store the data in a single Amazon S3 bucket. Write a bucket policy that uses conditions to grant read and write access where appropriate, based on each user's business unit and job type. Determine the business unit with the AWS account accessing the bucket and the job type with a prefix in the IAM user's name. Users can access data by using IAM credentials from their business unit's AWS account with an S3 client.

C. Store the data in a series of Amazon S3 buckets. Create an application running in Amazon EC2 that is integrated with the company's identity provider (IdP) that authenticates users and allows them to download or upload data through the application. The application uses the business unit and job type information in the IdP to control what users can upload and download through the application. The users can access the data through the application's API.

D. Store the data in a series of Amazon S3 buckets. Create an AWS STS token vending machine that is integrated with the company's identity provider (IdP). When a user logs in, have the token vending machine attach an IAM policy that assumes the role that limits the user's access and/or upload only the data the user is authorized to access. Users can get credentials by authenticating to the token vending machine's website or API and then use those credentials with an S3 client.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.For best practice, we should use IAM Role. However, this solution will mean every time an account get added, we will need to create role for all job type in the account, and in the account we need to attach IAM policies to prevent them assume other job type roles. This could be a lot of work.
B.his is not the ideal solution, but it requires minimal effort when we add or remove an account. We could use deny rule to achieve this by deny account or job type not in a list. 10PB in a single bucket seems too much and we need to update the policy every time a new company joins.

C.Too much overhead.
D.token vending machine  is majorly used by mobile app and I don't think it is a good solution here. However, in terms of management, I think this is the best solution

**QUESTION 82**
A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege. A Solutions Architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster.
What steps are required after the deployment to meet the requirements? (Choose 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.

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.As in bridge mode all containers in the same instance share the same security group of the instance, we could open ports that are not necessary. This is not good for least privilege.
B.As each task gets its own ENI and security group, we could do fine grained permission here
C.If we don't pick A, this is not necessary
D.Pass IAM credential is bad practice
E.https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html

**QUESTION 83**
A company is migrating its marketing website and content management system from an onpremises data center to AWS. The company wants the AWS application to be developed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database. The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers. After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.
How can the application and environment be deployed and automated in AWS, while allowing for future changes?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Not the best solution
B.Cloudformation is a better choice
C.We could automate the rest of the steps
D.https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html

**QUESTION 84**
A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4. Company policy requires systems that communicate with external vendors use a security group that limits access to only approved external vendors. The virtual private cloud (VPC) uses the default network ACL. The Systems Operator successfully assigns IPv6 addresses to each of the backend systems. The Systems Operator also updates the outbound security group to include the IPv6 CIDR of the external vendor (destination). The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor. What changes are required to enable communication with the external vendor?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
IPv6 is not supported by Nat gateway or Nat instance
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html
https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

**QUESTION 85**
A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand. Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

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.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 86**
A Solutions Architect is designing the storage layer for a data warehousing application. The data files are large, but they have statically placed metadata at the beginning of each file that describes the size and

placement of the file's index. The data files are read in by a fleet of Amazon EC2 instances that store the index size, index location, and other category information about the data file in a database. That database is used by Amazon EMR to group files together for deeper analysis. What would be the MOST cost-effective, high availability storage solution for this workflow?

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
S3 object data will be a good fit here as we do not need to load the file for metadata information as we can do range get.
https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectGET.html

**QUESTION 87**
A company uses an Amazon EMR cluster to process data once a day. The raw data comes from Amazon S3, and the resulting processed data is also stored in Amazon S3. The processing must complete within 4 hours; currently, it only takes 3 hours. However, the processing time is taking 5 to 10 minutes. longer each week due to an increasing volume of raw data. The team is also concerned about rising costs as the compute capacity increases. The EMR cluster is currently running on three m3 xlarge instances (one master and two core nodes).
Which of the following solutions will reduce costs related to the increasing compute needs?

A. Add additional task nodes, but have the team purchase an all-upfront convertible Reserved Instance for each additional node to offset the costs.
B. Add additional task nodes, but use instance fleets with the master node in on-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase a scheduled Reserved Instances for the master node.
C. Add additional task nodes, but use instance fleets with the master node in Spot mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase enough scheduled Reserved Instances to offset the cost of running any On-Demand instances.
D. Add additional task nodes, but use instance fleets with the master node in On-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase a standard allupfront Reserved Instance for the master node.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Spot instance will be cheaper
C.Master node should not be spot instance
D.All upfront should be more expensive than scheduled reserved instnace

**QUESTION 88**
A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications.
Which solution meets the requirements by using the LEAST amount of management overhead?

A. Connect the Active Directory to AWS by using single sign-on and an Active Directory Federation Services (AD FS) with SAML 2.0, and then configure the identity Provider (IdP) system to use

formbased 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 third-party single sign-on as needed, and add it to the AD FS server.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will work but you will need to build login page in your on-prem environment and AD FS portal page and the AD FS server
C.I don't think service linking function is used in this way.
We should use AWS SSO for federations so that we could leverage third-party SSO.
https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html
https://aws.amazon.com/blogs/security/how-to-create-and-manage-users-within-aws-sso/
D.Will need to maintain the AD FS server

**QUESTION 89**
A Solutions Architect is designing a network solution for a company that has applications running in a data center in Northern Virginia. The applications in the company's data center require predictable performance to applications running in a virtual private cloud (VPC) located in us-east-1, and a secondary VPC in us-west-2 within the same account. The company data center is collocated in an AWS Direct Connect facility that serves the us-est-1 region. The company has already ordered an AWS Direct Connect connection and a cross-connect has been established.
Which solution will meet the requirements at the LOWEST cost?

A. Provision a Direct Connect gateway and attach the virtual private (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 partner to establish a network extension link over dark fiber from the Direct Connect facility to the company's data center. Establish private VIFs on the Direct Connect connections for each of the company's VPCs in the respective regions.
Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFs.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Direct Connect Gateway is global resource, which makes connect to other region fast as well
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html
B.A is better as less latency
https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/
C.I don't we think we need public VIF here. Also, maintaining a EC2 server is overhead.
D.This will work, but A is much cheaper

**QUESTION 90**
A company has a web service deployed in the following two AWS Regions: us-west-2 and us-east-1. Each AWS region runs an identical version of the web service. Amazon Route 53 is used to route customers to the AWS Region that has the lowest latency. The company wants to improve the availability of the web service in case an outage occurs in one of the two AWS Regions.
A Solutions Architect has recommended that a Route 53 health check be performed. The health check must detect a specific text on an endpoint. What combination of conditions should the endpoint meet to pass the Route 53 health check? (Choose 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.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.The limit is 4 seconds
B.2xx or 3xx is good.
E.Must response within 2 seconds
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html#dns-failover-determining-health-of-endpoints-monitor-endpoint

**QUESTION 91**
A company operating a website on AWS requires high levels of scalability, availability and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage Amazon CloudFront is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution.
Which solution is the MOST cost-effective at scale?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Database with EC2 is expensive, and EBS has maximum size of 16TB
B.Aurora storage can sacale automatically

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Performance.html#Aurora.Managing.Performance.StorageScaling
D.Aurora storage can sacale automatically

**QUESTION 92**
The Security team needs to provide a team of interns with an AWS environment so they can build the serverless video transcoding application. The project will use Amazon S3, AWS Lambda, Amazon API Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder.
The interns should be able to create and configure the necessary resources, but they may not have access to create or modify AWS IAM roles. The Solutions Architect creates a policy and attaches it to the interns' group.
How should the Security team configure the environment to ensure that the interns are selfsufficient?

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Intern should not have access to IAM
C.This just won't work. Some of the mentioned resources are global resources and they do not belong to a subnet or a VPC, and you will need IAM to do this, not just a bastion server.
D.Raise request is not self sufficient

**QUESTION 93**
A company is running a commercial Apache Hadoop cluster on Amazon EC2. This cluster is being used daily to query large files on Amazon S3. The data on Amazon S3 has been curated and does not require any additional transformations steps. The company is using a commercial business intelligence (BI) tool on Amazon EC2 to run queries against the Hadoop cluster and visualize the data.
The company wants to reduce or eliminate the overhead costs associated with managing the Hadoop cluster and the BI tool. The company would like to remove to a more cost-effective solution with minimal effort. The visualization is simple and requires performing some basic aggregation steps only.
Which option will meet the company's requirements?

A. Launch a transient Amazon EMR cluster daily and develop an Apache Hive script to analyze the files on Amazon S3. Shut down the Amazon EMR cluster when the job is complete. The use the Amazon QuickSight to connect to Amazon EMR and perform the visualization.
B. Develop a stored procedure invoked from a MySQL database running on Amazon EC2 to analyze EC2 to analyze the files in Amazon S3. Then use a fast in-memory BL tool running on Amazon EC2 to visualize the data.
C. Develop a script that uses Amazon Athena to query and analyze the files on Amazon S3.
Then use Amazon QuickSight to connect to Athena and perform the visualization.
D. Use a commercial extract, transform, load (ETL) tool that runs on Amazon EC2 to prepare the data for processing. Then switch to a faster and cheaper BI tool that runs on Amazon EC2 to visualize the data from Amazon S3.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This could work but EMR spin up daily still expensive. Also, to connect quicksight to EMR you will need

presto running in the cluster...
B.this is just bad...and I do not think you can access s3 from a stored proc...
D.Bad practice...ETL could take very long time...

**QUESTION 94**
A large multinational company runs a timesheet application on AWS that is used by staff across the world. The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer, and stores in an Amazon RDS MySQL Multi-AZ database instance.
The CFO is concerned about the impact on the business if the application is not available. The application must not be down for more than two hours, but he solution must be as cost-effective as possible.
How should the Solutions Architect meet the CFO's requirements while minimizing data loss?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Multi site is expensive and we probably do not need it for 2 hour RTO
B.Under the hood, snapshot is regional resource, you will need to copy to other region to use it.
C.Compare to D, there could be 1 hour data lost.
D.This is a typical pilot light structure and almost had no data lost

**QUESTION 95**
A development team has created a series of AWS CloudFormation templates to help deploy services. They created a template for a network/virtual private (VPC) stack, a database stack, a bastion host stack, and a web application-specific stack. Each service requires the deployment of at least:
* A network/VPC stack
* A bastion host stack
* A web application stack
Each template has multiple input parameters that make it difficult to deploy the services individually from the AWS CloudFormation console. The input parameters from one stack are typically outputs from other stacks. For example, the VPC ID, subnet IDs, and security groups from the network stack may need to be used in the application stack or database stack.
Which actions will help reduce the operational burden and the number of parameters passed into a service deployment? (Choose two.)

A. Create a new AWS CloudFormation template for each service. After 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 dependences 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. After 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. After the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Create a product for each application. Add the service template to the product. Add each new product to the portfolio.
Deploy the product from the portfolio to deploy the service with the necessary parameters only to start the deployment.

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Cloudformation console is not very good to handle multiple services
B.A service should not be a portfolio, it is more like a product. Also, I don't think it is possible to launch a portfolio
C.Use CodePipeline is good, but I am not comfortable to share parameter with config files and scripts. We still could use cross-stack reference for this, but this is one of the best two
D.You can't deploy a cloudformation template directly from Step Function
https://docs.aws.amazon.com/step-functions/latest/dg/concepts-service-integrations.html
E.A nested stack with cross stack reference example
https://cloudacademy.com/blog/understanding-nested-cloudformation-stacks/

**QUESTION 96**
A company has an application behind a load balancer with enough Amazon EC2 instances to satisfy peak demand. Scripts and third-party deployment solutions are used to configure EC2 instances when demand increases or an instance fails. The team must periodically evaluate the utilization of the instance types to ensure that the correct sizes are deployed. How can this workload be optimized to meet these requirements?

A. Use CloudFormer` to create AWS CloudFormation stacks from the current resources.
Deploy that stack by using AWS CloudFormation in the same region. Use Amazon CloudWatch alarms to send notifications about underutilized resources to provide cost-savings suggestions.

B. Create an Auto Scaling group to scale the instances, and use AWS CodeDeploy to perform the configuration. Change from a load balancer to an Application Load Balancer. Purchase a third-party product that provides suggestions for cost savings on AWS resources.

C. Deploy the application by using AWS Elastic Beanstalk with default options. Register for an AWS Support Developer plan. Review the instance usage for the application by using Amazon CloudWatch, and identify less expensive instances that can handle the load. Hold monthly meetings to review new instance types and determine whether Reserved instances should be purchased.

D. Deploy the application as a Docker image by using Amazon ECS. Set up Amazon EC2 Auto Scaling and Amazon ECS scaling. Register for AWS Business Support and use Trusted Advisor checks to provide suggestions on cost savings.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.We don't need cloudformation here
B.CodeDeploy is not really used to config infrastructures (config auto scale group)
C.This answer solve nothing…..

**QUESTION 97**
A large global financial services company has multiple business units. The company wants to allow Developers to try new services, but there are multiple compliance requirements for different workloads. The Security team is concerned about the access strategy for on-premises and AWS implementations. They would like to enforce governance for AWS services used by business team for regulatory workloads, including Payment Card Industry (PCI) requirements.
Which solution will address the Security team's concerns and allow the Developers to try new services?

A. Implement a strong identity and access management model that includes users, groups, and roles in various AWS accounts. Ensure that centralized AWS CloudTrail logging is enabled to detect anomalies. Build automation with AWS Lambda to tear down unapproved AWS resources for governance.
B. Build a multi-account strategy based on business units, environments, and specific regulatory requirements. Implement SAML-based federation across all AWS accounts with an on-premises identity store. Use AWS Organizations and build organizational units (OUs) structure based on regulations and service governance. Implement service control policies across OUs.
C. Implement a multi-account strategy based on business units, environments, and specific regulatory requirements. Ensure that only PCI-compliant services are approved for use in the accounts. Build IAM policies to give access to only PCI-compliant services for governance.
D. Build one AWS account for the company for the strong security controls. Ensure that all the service limits are raised to meet company scalability requirements. Implement SAML federation with an on-premises identity store, and ensure that only approved services are used in the account.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Should try to stop service get created at the first place
C.SCP is better fit here?
D.Not the best practice

**QUESTION 98**
A company had a tight deadline to migrate its on-premises environment to AWS. It moved over Microsoft SQL Servers and Microsoft Windows Servers using the virtual machine import/export service and rebuild other applications native to the cloud. The team created both Amazon EC2 databases and used Amazon RDS. Each team in the company was responsible for migrating their applications, and would like suggestions on reducing its AWS spend.
Which steps should a Solutions Architect take to reduce costs?

A. Enable AWS Business Support and review AWS Trusted Advisor's cost checks. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand. Save AWS Simple Monthly Calculator reports in Amazon S3 for trend analysis. Create a master account under Organizations and have teams join for consolidating billing.
B. Enable Cost Explorer and AWS Business Support Reserve Amazon EC2 and Amazon RDS DB instances. Use Amazon CloudWatch and AWS Trusted Advisor for monitoring and to receive costsavings suggestions. Create a master account under Organizations and have teams join for consolidated billing.
C. Create an AWS Lambda function that changes the instance size based on Amazon CloudWatch alarms. Reserve instances based on AWS Simple Monthly Calculator suggestions. Have an AWS Well-Architected framework review and apply recommendations.
Create a master account under Organizations and have teams join for consolidated billing.
D. Create a budget and monitor for costs exceeding the budget. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand. Create an AWS Lambda function that changes instance sizes based on Amazon CloudWatch alarms. Have each team upload their bill to an Amazon S3 bucket for analysis of team spending. Use Spot instances on nightly batch processing jobs.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

A.Simple monthly  aculator report is not really a report for analysis trends .
C.Resize instance may require stop the instance first, which is not ideal for production environments….
D.Consolidate billing is a must, this is out

**QUESTION 99**
A company wants to replace its call system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the callers and handle basic tasks, reducing the need to speak an agent. The solution should also be able to query business applications and provide relevant information back to calls as requested. Which services should the Solution Architect use to build this solution? (Choose three.)

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

**Correct Answer:** BDE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Recognition is for image and video
B.Amazon connect is a call centre service
C.Alexa is for devices
E.Lex is used to build conversational interface
F.Caller queue is manage by Amazon connect as well, and SQS is not designed for this.

**QUESTION 100**
A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon. The Finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs. The Security team requires a centralized mechanism to control IAM usage in all the company's accounts. What combination of the following options meet the company's needs with LEAST effort? (Choose two.)

A. Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.
B. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.
C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.
D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.
E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and IAM's Access Advice feature to enforce the least privilege model.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will work, but the process will have a bit effort.
C.We will like consolidate billing as well...
D.https://aws.amazon.com/blogs/security/how-to-use-service-control-policies-to-set-permission-guardrails-across-accounts-in-your-aws-organization/
E.Single account is not a good option

**QUESTION 101**
A company collects a steady stream of 10 million data records from 100,000 sources each day. These records are written to an Amazon RDS MySQL DB. A query must produce the daily average of a data source over the past 30 days. There are twice as many reads as writes. Queries to the collected data are for one source ID at a time. How can the Solutions Architect improve the reliability and cost effectiveness of this solution?

A. Use Amazon Aurora with MySQL in a Multi-AZ mode. Use four additional read replicas.
B. Use Amazon DynamoDB with the source ID as the partition key and the timestamp as the sort key. Use a Time to Live (TTL) to delete data after 30 days.
C. Use Amazon DynamoDB with the source ID as the partition key. Use a different table each day.
D. Ingest data into Amazon Kinesis using a retention period of 30 days. Use AWS Lambda to write data records to Amazon ElastiCache for read access.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Cheapest and can do the job.
D.Most expensive one.

**QUESTION 102**
A company is moving a business-critical application onto AWS. It is a traditional threetier web application using an Oracle database. Data must be encrypted in transit and at rest. The database hosts 12 TB of data. Network connectivity to the source Oracle database over the internal is allowed, and the company wants to reduce the operational costs by using AWS Managed Services where possible. All primary keys only; however, it contains many Binary Large Object (BLOB) fields. It was not possible to use the database's native replication tools because of licensing restrictions.
Which database migration solution will result in the LEAST amount of impact to the application's availability?

A. Provision an Amazon RDS for Oracle instance. Host the RDS database within a virtual private cloud (VPC) subnet with internet access, and set up the RDS database as an encrypted Read Replica of the source database. Use SSL to encrypt the connection between the two databases. Monitor the replication performance by watching the RDS ReplicaLag metric. During the application maintenance window, shut down the on-premises database and switch over the application connection to the RDS instance when there is no more replication lag. Promote the Read Replica into a standalone database instance.
B. Provision an Amazon EC2 instance and install the same Oracle database software. Create a backup of the source database using the supported tools. During the application maintenance window, restore the backup into the Oracle database running in the EC2 instance. Set up an Amazon RDS for Oracle instance, and create an import job between the database hosted in AWS. Shut down the source database and switch over the database connections to the RDS instance when the job is complete.
C. Use AWS DMS to load and replicate the dataset between the on-premises Oracle database and the replication instance hosted on AWS. Provision an Amazon RDS for Oracle instance with Transparent Data Encryption (TDE) enabled and configure it as target for the replication instance. Create a customer-managed AWS KMS master key to set it as the encryption key for the replication instance. Use AWS DMS tasks to load the data into the target RDS instance. During the application maintenance window and after the load tasks reach the ongoing replication phase, switch the database connections to the new database.
D. Create a compressed full database backup on the on-premises Oracle database during an application maintenance window. While the backup is being performed, provision a 10 Gbps AWS Direct Connect connection to increase the transfer speed of the database backup files to Amazon S3, and shorten the maintenance window period. Use SSL/TLS to copy the files over the Direct Connect connection. When the backup files are successfully copied, start the maintenance window, and rise any of the Amazon RDS supported tools to import the data into a newly provisioned Amazon RDS for Oracle instance with encryption enabled. Wait until the data is fully loaded and switch over the database connections to the new database.
Delete the Direct Connect connection to cut unnecessary charges.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Best solution, but native replication cannot be used
B.Backup may not contain most up to date data
C.You cannot use a KMS key for TDE encryption, but we are encrypted the replication instance with KMS and use TDE for newly created RDS instance.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.Oracle.html
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.SQLServer.html
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_ReplicationInstance.html
D.This will take hours when migrate

**QUESTION 103**
A company has detected to move some workloads onto AWS to create a grid environment to run market analytics. The grid will consist of many similar instances, spun-up by a job-scheduling function. Each time a large analytics workload is completed, a new VPC is deployed along with job scheduler and grid nodes. Multiple grids could be running in parallel.
Key requirements are:
* Grid instances must communicate with Amazon S3 retrieve data to be processed.
* Grid instances must communicate with Amazon DynamoDB to track intermediate data,
* The job scheduler need only to communicate with the Amazon EC2 API to start new grid nodes.
A key requirement is that the environment has no access to the internet, either directly or via the onpremises proxy. However, the application needs to be able to seamlessly communicate to Amazon S3, Amazon DynamoDB, and Amazon EC2 API, without the need for reconfiguration for each new deployment.
Which of the following should the Solutions Architect do to achieve this target architecture? (Choose three.)

A. Enable VPC endpoints for Amazon S3 and DynamoDB.
B. Disable Private DNS Name Support.
C. Configure the application on the grid instances to use the private DNS name of the Amazon S3 endpoint.
D. Populate the on-premises DNS server with the private IP addresses of the EC2 endpoint.
E. Enable an interface VPC endpoint for EC2.
F. Configure Amazon S3 endpoint policy to permit access only from the grid nodes.



**Correct Answer:** ADE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html
B.Private DNS is needed for interface VPC endpoint
C.S3 endpoint is gateway endpoint
Private DNS name of s3 endpoint is not a thing. You will need to use prefix list ID for the route table and continue to use the S3 DNS name for the service
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html#vpc-endpoints-routing
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html
D.This is necessary as the default EC2 endpoint route is only populated in VPC route table, and private IP for interface endpoint DNS name is required in the DNS server.
E.https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html
F.S3 is gateway endpoint and you cannot limit principal in the endpoint policy
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-access.html#vpc-endpoint-policies

**QUESTION 104**
An internal security audit of AWS resources within a company found that a number of Amazon EC2 instances running Microsoft Windows workloads were missing several important operating system-level patches. A Solutions Architect has been asked to fix existing patch deficiencies, and to develop a workflow to ensure that future patching requirements are identified and taken care of quickly. The Solutions Architect has decided to use AWS Systems Manager. It is important that EC2 instance reboots do not occur at the same time on all Windows workloads to meet organizational uptime requirements. Which workflow will meet these requirements in an automated manner?

A. Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline to the Windows servers patch group. Define an AWS Systems Manager maintenance window, conduct patching within it, and associate it with the Windows Servers patch group. Register instances with the maintenance window using associated subnet IDs. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.

B. Add a Patch Group tag a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-WindowsPatchBaseline document as a task associated with the Windows Servers patch group. Create an Amazon CloudWatch Events rule configured to use a cron expression to schedule the execution of patching using the AWS Systems Manager run command. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.

C. Add a Patch Group tag with a value of either Windows Servers1 or Windows Server2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag.
Associate the AWSDefaultPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Register targets with specific maintenance windows using the Patch Group tags. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.

D. Add a Patch Group tag with a value of either Windows servers1 or Windows Server2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag.
Associate the AWSWindowsPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Assign the AWS-RunWindowsPatchBaseline document as a task within each maintenance window.
Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.All instances will be patched at the same time, down time
B.AWS-WindowsPatchBaseline is not a valid one
Also when using patch group, you don't use run command
C.https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-scheduletasks.html
https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-patchgroups.html
D.AWS-WindowsPatchBaseline is not a valid one
https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html

**QUESTION 105**
A company must deploy multiple independent instances of an application. The front-end application is internet accessible. However, corporate policy stipulates that the backends are to be isolated from each other and the internet, yet accessible from a centralized administration server. The application setup should be automated to minimize the opportunity for mistakes as new instances are deployed. Which option meets the requirements and MINIMIZES costs?

A. Use an AWS CloudFormation template to create identical IAM roles for each region. Use AWS CloudFormation StackSets to deploy each application instance by using parameters to customize for each instance, and use security groups to isolate each instance while permitting access to the central server.

B. Create each instance of the application IAM roles and resources in separate accounts by using AWS CloudFormation StackSets. Include a VPN connection to the VPN gateway of the central administration server.

C. Duplicate the application IAM roles and resources in separate accounts by using a single CloudFormation template. Include VPC peering to connect the VPC of each application instance to a central VPC.

D. Use the parameters of the AWS CloudFormation template to customize the deployment into separate accounts. Include a NAT gateway to allow communication back to the central administration server.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Security group will not applied to newly created instance
B.https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-vpn-gateway.html
C.You cannot use a single cloudformation template to create resources across account
D.NAT gateway will access the internet

**QUESTION 106**
A group of Amazon EC2 instances have been configured as high performance computing (HPC) cluster. The instances are running in a placement group, and are able to communicate with each other at network of up to 20 Gbps. The cluster needs to communicate with a control EC2 instance outside of the placement group. The control instance has the same instance type and AMI as the other instances, and is configured with a public IP address.
How can the Solutions Architect improve the network speeds between the control instance and the instances in the placement group?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
The HPC is already running with ENA as it had up to 20 Gbps connection already. All we need to do is move the control instance into the placement group. Also, ENA should be enabled automatically for supported kernel and instance type, so C is not correct.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#change-instance-placement-group
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
https://aws.amazon.com/blogs/aws/elastic-network-adapter-high-performance-network-interface-for-amazon-ec2/
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html

**QUESTION 107**
A Solutions Architect has created an AWS CloudFormation template for a three-tier application that contains an Auto Scaling group of Amazon EC2 instances running a custom AMI. The Solutions Architect wants to ensure that future updates to the custom AMI can be deployed to a running stack by first updating the template to refer to the new AMI, and then invoking UpdateStack to replace the EC2 instances with instances launched from the new AMI.
How can updates to the AMI be deployed to meet these requirements?

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 to Replace. DeletionPolicy
C. Edit the AWS::AutoScaling: :LaunchConfiguration resource in the template, inserting an attribute. UpdatePolicy
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.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

A.Old Instance is not going to be updated
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/updating.stacks.walkthrough.html#update.walkthrough.ami
B.DeletionPolicy is for behaviour after deletion
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html
C.https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-updatepolicy.html
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as-launchconfig.html

**QUESTION 108**
A Solutions Architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements:
* Consolidate all accounts into one organization.
* Allow full access to the Amazon EC2 service from the master account and the secondary accounts.
* Minimize the effort required to add additional secondary accounts. Which combination of steps should be included in the solution? (Choose two.)

A. Create an organization from the master account. Send invitations to the secondary accounts from the master account. Accept the invitations and create an OU.
B. Create an organization from the master account. Send a join request to the master account from each secondary account. Accept the requests and create an OU.
C. Create a VPC peering connection between the master account and the secondary accounts. Accept the request for the VPC peering connection.
D. Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU.
E. Create a full EC2 access policy and map the policy to a role in each account. Trust every other account to assume the role.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_invites.html

**QUESTION 109**
AnyCompany has acquired numerous companies over the past few years. The CIO for AnyCompany would like to keep the resources for each acquired company separate. The CIO also would like to enforce a chargeback model where each company pays for the AWS services it uses The Solutions Architect is tasked with designing an AWS architecture that allows AnyCompany to achieve the following:
* Implementing a detailed chargeback mechanism to ensure that each company pays for the resources it uses.
* AnyCompany can pay for AWS services for all its companies through a single invoice.
* Developers in each acquired company have access to resources in their company only.
* Developers in an acquired company should not be able to affect resources in their company only.
* A single identity store is used to authenticate Developers across all companies. Which of the following approaches would meet these requirements? (Choose two.)

A. Create a multi-account strategy with an account per company. Use consolidated billing to ensure that AnyCompany needs to pay a single bill only.
B. Create a multi-account strategy with a virtual private cloud (VPC) for each company.
Reduce impact across companies by not creating any VPC peering links. As everything is in a single account, there will be a single invoice. use tagging to create a detailed bill for each company.
C. Create IAM users for each Developer in the account to which they require access. Create policies that allow the users access to all resources in that account. Attach the policies to the IAM user.
D. Create a federated identity store against the company's Active Directory. Create IAM roles with appropriate permissions and set the trust relationships with AWS and the identity store.
Use AWS STS to grant users access based on the groups they belong to in the identity store.
E. Create a multi-account strategy with an account per company. For billing purposes, use a tagging solution that uses a tag to identify the company that creates each resource.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
https://aws.amazon.com/blogs/security/how-to-set-up-uninterrupted-federated-user-access-to-aws-using-ad-fs/

**QUESTION 110**
A company deployed a three-tier web application in two regions: us-east-1 and eu-west-1. The application must be active in both regions at the same time. The database tier of the application uses a single Amazon RDS Aurora database globally, with a master in us-east-1 and a read replica in eu-west-1. Both regions are connected by a VPN. The company wants to ensure that the application remains available even in the event of a regionlevel failure of all of the application's components. It is acceptable for the application to be in readonly mode for up to 1 hour. The company plans to configure two Amazon Route 53 record sets, one for each of the regions. How should the company complete the configuration to meet its requirements while providing the lowest latency for the application end-users? (Choose two.)

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

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.This will not ensure low latency for all requests
B.This will not ensure low latency
C.Latency routing also supports failover
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html
D.Healthy check fails doesn't mean database fails

**QUESTION 111**
A company runs a Windows Server host in a public subnet that is configured to allow a team of administrators to connect over RDP to troubleshoot issues with hosts in a private subnet. The host must be available at all times outside of a scheduled maintenance window, and needs to receive the latest operating system updates within 3 days of release. What should be done to manage the host with the LEAST amount of administrative effort?

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

A.Should not use SSM to manage EB instance.
B.https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html
C.This could work, but it is hard to manage as instance could be replaced by the auto scale group and SMS will not be able to track.
D.upgrade operation system only works for Linux
https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks-commands.html

**QUESTION 112**
A company has a large on-premises Apache Hadoop cluster with a 20 PB HDFS database. The cluster is growing every quarter by roughly 200 instances and 1 PB. The company's goals are to enable resiliency for its Hadoop data, limit the impact of losing cluster nodes, and significantly reduce costs. The current cluster runs 24/7 and supports a variety of analysis workloads, including interactive queries and batch processing.
Which solution would meet these requirements with the LEAST expense and down time?

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Purchase additional RI quarterly won't help auto scale with interactive queries and batch processing
C.AWS suggest use snowmobile for data larger than 10PB
D.Direct connect will take years

**QUESTION 113**
A company is running a large application on-premises. Its technology stack consists of Microsoft .NET for the web server platform and Apache Cassandra for the database. The company wants to migrate the application to AWS to improve service reliability. The IT team also wants to reduce the time it spends on capacity management and maintenance of this infrastructure. The Development team is willing and available to make code changes to support the migration.
Which design is the LEAST complex to manage after the migration?

A. Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running .NET. Migrate the existing Cassandra database to Amazon Aurora with multiple read replicas, and run both in a Multi-AZ mode.
B. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the .NET platform in a Multi-AZ Auto Scaling configuration. Migrate the Cassandra database to Amazon EC2 instances that are running in a Multi-AZ configuration.
C. Migrate the web servers to an AWS Elastic Beanstalk environment that is running the .NET platform in a Multi-AZ Auto Scaling configuration. Migrate the existing Cassandra database to Amazon DynamoDB.

D. Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running .NET. Migrate the existing Cassandra database to Amazon DynamoDB.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.EC2
B.EC2 database is not good
D.EC2 has more management cost

**QUESTION 114**
A company has a requirement that only allows specially hardened AMIs to be launched into public subnets in a VPC, and for the AMIs to be associated with a specific security group. Allowing non-compliant instances to launch into the public subnet could present a significant security risk if they are allowed to operate. A mapping of approved AMIs to subnets to security groups exists in an Amazon DynamoDB table in the same AWS account. The company created an AWS Lambda function that, when invoked, will terminate a given Amazon EC2 instance if the combination of AMI, subnet, and security group are not approved in the DynamoDB table.
What should the Solutions Architect do to MOST quickly mitigate the risk of compliance deviations?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Will not stop non compliance launched AMI
B.Cloudtrail logs has up to 5 to 15 mins to display
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/get-and-view-cloudtrail-log-files.html
C.Cloudtrail can monitor ec2:Runinstance api call, but Cloudtrail logs has up to 5 to 15 mins to display
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/using-cloudtrail.html
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/get-and-view-cloudtrail-log-files.html
D.https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/automating_with_cloudwatch_events.html

**QUESTION 115**
A Solutions Architect must migrate an existing on-premises web application with 70 TB of static files supporting a public open-data initiative. The architect wants to upgrade to the latest version of the host operating system as part of the migration effort. Which is the FASTEST and MOST cost-effective way to perform the migration?

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

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.P2V is not supported by Server migration service, and EC2
https://forums.aws.amazon.com/thread.jspa?messageID=794316&tstart=0
https://docs.aws.amazon.com/server-migration-service/latest/userguide/prereqs.html
B.P2V is not supported by Server migration service
D.SMS cannot update the OS

**QUESTION 116**
A company has an application that generates a weather forecast that is updated every 15 minutes with an output resolution of 1 billion unique positions, each approximately 20 bytes in size (20 Gigabytes per forecast). Every hour, the forecast data is globally accessed approximately 5 million times (1,400 requests per second), and up to 10 times more during weather events. The forecast data is overwritten every update. Users of the current weather forecast application expect responses to queries to be returned in less than two seconds for each request.
Which design meets the required request rate and response time?

A. Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Enable API caching on the API Gateway stage with a cache-control timeout set for 15 minutes.
B. Store forecast locations in an Amazon EFS volume. Create an Amazon CloudFront distribution that targets an Elastic Load Balancing group of an Auto Scaling fleet of Amazon EC2 instances that have mounted the Amazon EFS volume. Set the set cache-control timeout for 15 minutes in the CloudFront distribution.
C. Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Create an Amazon Lambda@Edge function that caches the data locally at edge locations for 15 minutes.
D. Store forecast locations in an Amazon S3 as individual objects. Create an Amazon CloudFront distribution targeting an Elastic Load Balancing group of an Auto Scaling fleet of EC2 instances, querying the origin of the S3 object. Set the cache-control timeout for 15 minutes in the 3CloudFront distribution.



**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.API gateway cache will be in the region of the API gateway
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html
Also, API gateway has request limits
https://docs.aws.amazon.com/apigateway/latest/developerguide/limits.html
B.Cache-control header is set in the origin, not cloudfront
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html
C.You don't need Lambda@Edge for cloudfront cache, but you can cache the data in lambda memory. However, for 20GB data, it will be too much…As you also use Lambda@Edge for cache, the hit rate will most likely exceed the concurrent limit
https://aws.amazon.com/blogs/networking-and-content-delivery/leveraging-external-data-in-lambdaedge/
https://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge-design-best-practices/
D.Cache-control header is set in the origin, not cloudfront
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html

**QUESTION 117**
A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that, if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted. How can the company prevent users from accidentally deleting data in this way?

A. Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.
B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
C. Modify IAM policies to deny deleting RDS an EBS resources that are tagged with an

"aws:cloudformation:stackname" tag.

D. Use AWS Config rules to prevent deleting RDS and EBS resources.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.https://aws.amazon.com/premiumsupport/knowledge-center/delete-cf-stack-retain-resources/
B.Stack Policy is used when stack is updated
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html
C.This will prevent deletion that are on purpose
D.Config rule is used to monitor, not prevention

**QUESTION 118**
A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda and Amazon DynamoDB. They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept Amazon CloudWatch metrics did not indicate any issues with DynamoDB but showed that some Lambda functions were hitting their timeout. Which of the following actions should the Solutions Architect consider to improve performance? (Choose two.)

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



**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.No such thing, this is automatic
C.This won't help much

**QUESTION 119**
A company is using AWS to run an internet-facing production application written in Node.js. The Development team is responsible for pushing new versions of their software directly to production. The application software is updated multiple times a day. The team needs guidance from a Solutions Architect to help them deploy the software to the production fleet quickly and with the least amount of disruption to the service.
Which option meets these requirements?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.AMI should be the baseline
B.CodeDeploy cannot deploy AMI
C.Manaul work involved

**QUESTION 120**
A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume. The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos. Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Not going to help much as EC2 maybe the bottleneck
B.Data lost when accident happens
D.Still using the EC2 to serve

**QUESTION 121**
A company runs its containerized batch jobs on Amazon ECS. The jobs are scheduled by submitting a container image, a task definition, and the relevant data to an Amazon S3 bucket. Container images may be unique per job. Running the jobs as quickly as possible is of utmost importance, so submitting jobs artifacts to the S3 bucket triggers the job to run immediately. Sometimes there may no jobs running at all. However, jobs of any size can be submitted with no prior warning to the IT Operations team. Job definitions include CPU and memory resource requirements.
What solution will allow the batch jobs to complete as quickly as possible after being scheduled?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.EC2 size will be the limit of the job resource
B.EC2 size will be the limit of the job resource. Also we cannot determine the base line as any size of the job can be submitted
C.Fargate will be the option here as the job can be started immediately and it can run jobs without limit of the EC2 size
D.Fargate has nothing to do with spot instance, also spot instance may not be available at the time of request

**QUESTION 122**

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

A. Increase the size of the instance to speed up processing and update the schedule to run once an hour.
B. Convert the cron job to an AWS Lambda function and trigger this new function using a cron job on an EC2 instance.
C. Convert the cron job to an AWS Lambda function and schedule it to run once an hour using Amazon CloudWatch events.
D. Create an AWS Lambda function that runs when a file is delivered to Amazon S3 using S3 event notifications.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 123**
A company that is new to AWS reports it has exhausted its service limits across several accounts that are on the Basic Support plan. The company would like to prevent this from happening in the future.
What is the MOST efficient way of monitoring and managing all service limits in the company's accounts?

A. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, provide notifications using Amazon SNS if the limits are close to exceeding the threshold.
B. Reach out to AWS Support to proactively increase the limits across all accounts. That way, the customer avoids creating and managing infrastructure just to raise the service limits.
C. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, programmatically increase the limits that are close to exceeding the threshold.
D. Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, and use Amazon SNS for notifications if a limit is close to exceeding the threshold. Ensure that the accounts are using the AWS Business Support plan at a minimum.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
To use service limit with cloudwatch you will need business plan
https://aws.amazon.com/about-aws/whats-new/2017/11/aws-trusted-advisor-adds-service-limit-dashboard-and-cloudwatch-metrics/
https://aws.amazon.com/blogs/mt/monitoring-service-limits-with-trusted-advisor-and-amazon-cloudwatch/

**QUESTION 124**
A company needs to run a software package that has a license that must be run on the same physical host for the duration of its use. The software package is only going to be used for 90 days. The company requires patching and restarting of all instances every 30 days.
How can these requirements be met using AWS?

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

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**
A.Auto placement is a setting for dedicated host, not dedicated instance, and you cannot guarantee to deploy instance to the same host after restart
B.https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-dedicated-hosts-work.html
C.The best you can do is reserve in an AZ, not hardware...
D.This is just wrong...

**QUESTION 125**
A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume. The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency. Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)

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

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Resize to 6TB will change the IOPS performance from 12288 to 16000, but 16000 will be the maximum IO a general pupose ssd (gp2) can get to. Therefore, this will not solve the issue permanently.
B.Theoretically Aurora should not have IOPS issue, however it still have maximum size limit of 64TB
C.A stream is good fit for data processing like this
D.Dynamo has no maximum data size limit, which is a good fit for this

**QUESTION 126**
A Solutions Architect is designing a system that will collect and store data from 2,000 internetconnected sensors. Each sensor produces 1 KB of data every second. The data must be available for analysis within a few seconds of it being sent to the system and stored for analysis indefinitely.
Which is the MOST cost-effective solution for collecting and storing the data?

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.We could use kinesis firehose data transformation to do the grouping, but the answer did not mention it

so grouping not possible. Also, firehose price could be very high as it charged for minimum 5 KB
https://docs.aws.amazon.com/firehose/latest/dev/data-transformation.html
C.It will be hard to group records with stream
D.It won't help much as the S3 IA has minimum billed size of 128 KB

**QUESTION 127**
An auction website enables users to bid on collectible items. The auction rules require that each bid is processed only once and in the order it was received. The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis Data Streams. A single t2.large instance has a cron job that runs the bid processor, which reads incoming bids from Kinesis Data Streams and processes each bid. The auction site is growing in popularity, but users are complaining that some bids are not registering. Troubleshooting indicates that the bid processor is too slow during peak demand hours, sometimes crashes while processing, and occasionally loses track of which records is being processed. What changes should make the bid processing more reliable?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.I don't think you can flag a record in Kinesis
B.Lambda has concurrent limit, and SNS cannot guarantee order
C.Not scalable but it is the best answer in here...For FIFO queue, we could actually have multiple consumers and use a message group id...
D.Scaling could help, but the bid processor may still crash and still cannot guarantee bid has been processed. (Kinesis don't have message level ack/fail)

**QUESTION 128**
A bank is re-architecting its mainframe-based credit card approval processing application to a cloud-native application on the AWS cloud. The new application will receive up to 1,000 requests per second at peak load. There are multiple steps to each transaction, and each step must receive the result of the previous step. The entire request must return an authorization response within less than 2 seconds with zero data loss. Every request must receive a response. The solution must be Payment Card Industry Data Security Standard (PCI DSS)-compliant.
Which option will meet all of the bank's objectives with the LEAST complexity and LOWEST cost while also meeting compliance requirements?

A. Create an Amazon API Gateway to process inbound requests using a single AWS Lambda task that performs multiple steps and returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application.
B. Create an Application Load Balancer with an Amazon ECS cluster on Amazon EC2 Dedicated instances in a target group to process incoming requests. Use Auto Scaling to scale the cluster out/in based on average CPU utilization. Deploy a web service that processes all of the approval steps and returns a JSON object with the approval status.
C. Deploy the application on Amazon EC2 on Dedicated Instances. Use an Elastic Load Balancer in front of a farm of application servers in an Auto Scaling group to handle incoming requests. Scale out/in based on a custom Amazon CloudWatch metric for the number of inbound requests per second after

measuring the capacity of a single instance.

D. Create an Amazon API Gateway to process inbound requests using a series of AWS Lambda processes, each with an Amazon SQS input queue. As each step completes, it writes its result to the next step's queue. The final step returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
This is the only one that guarantee 0 data loss

**QUESTION 129**
A Solutions Architect is migrating a 10 TB PostgreSQL database to Amazon RDS for PostgreSQL. The company's internet link is 50 MB with a VPN in the Amazon VPC, and the Solutions Architect needs to migrate the data and synchronize the changes before the cutover. The cutover must take place within an 8-day period. What is the LEAST complex method of migrating the database securely and reliably?

A. Order an AWS Snowball device and copy the database using the AWS DMS. When the database is available in Amazon 3, 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.



**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
The internet connection could take more than 8 days to migrate
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html

**QUESTION 130**
A Solutions Architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The Solutions Architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.
What should be done next to complete the update?

A. Redirect to the new environment using Amazon Route 53

B. Select the Swap Environment URLs option

C. Replace the Auto Scaling launch configuration

D. Update the DNS records to point to the green environment

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

**QUESTION 131**
A company has a legacy application running on servers on premises. To increase the application's reliability, the company wants to gain actionable insights using application logs. A Solutions Architect has

been given following requirements for the solution:
- Aggregate logs using AWS.
- Automate log analysis for errors.
- Notify the Operations team when errors go beyond a specified threshold.
What solution meets the requirements?

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.

**Correct Answer:** D
**Section: (none)**
**Explanation**

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

**QUESTION 132**
What combination of steps could a Solutions Architect take to protect a web workload running on Amazon EC2 from DDoS and application layer attacks? (Select 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.



**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/
C.WAF is not for auto scale group
E.https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html
Cloudfront, Route 53, AWS Shield and WAF are all mentioned in the blow document
https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/

**QUESTION 133**
A photo-sharing and publishing company receives 10,000 to 150,000 images daily. The company receives the images from multiple suppliers and users registered with the service. The company is moving to AWS and wants to enrich the existing metadata by adding data using Amazon Rekognition. The following is an example of the additional data:
As part of the cloud migration program, the company uploaded existing image data to Amazon S3 and told users to upload images directly to Amazon S3. What should the Solutions Architect do to support these requirements?

A. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon DynamoDB to store the metadata and Amazon ES to create an index. Use a web front-end to provide search capabilities backed by Amazon ES.
B. Use Amazon Kinesis to stream data based on an S3 event. Use an application running in Amazon EC2 to extract metadata from the images. Then store the data on Amazon DynamoDB and Amazon CloudSearch and create an index. Use a web front-end with search capabilities backed by CloudSearch.

C. Start an Amazon SQS queue based on S3 event notifications. Then have Amazon SQS send the metadata information to Amazon DynamoDB. An application running on Amazon EC2 extracts data from Amazon Rekognition using the API and adds data to DynamoDB and Amazon ES. Use a web front-end to provide search capabilities backed by Amazon ES.

D. Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon RDS MySQL Multi-AZ to store the metadata information and use Lambda to create an index. Use a web front-end with search capabilities backed by Lambda.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Kinesis cannot stream data from S3 event directly, and EC2 by itself is not the best scalable solution
C.SQS cannot send data to dynamodb directly, too many missing pieces here
D.Lambda cannot back a search, and MySQL is not the best to store metadata for search

**QUESTION 134**
A Solutions Architect is redesigning an image-viewing and messaging platform to be delivered as SaaS. Currently, there is a farm of virtual desktop infrastructure (VDI) that runs a desktop imageviewing application and a desktop messaging application. Both applications use a shared database to manage user accounts and sharing. Users log in from a web portal that launches the applications and streams the view of the application on the user's machine. The Development Operations team wants to move away from using VDI and wants to rewrite the application.
What is the MOST cost-effective architecture that offers both security and ease of management?

A. Run a website from an Amazon S3 bucket with a separate S3 bucket for images amd messaging data. Call AWS Lambda functions from embedded JavaScript to manage the dynamic content, and use Amazon Cognito for user and sharing management.

B. Run a website from Amazon EC2 Linux servers, storing the images in Amazon S3, and use Amazon Cognito for user accounts and sharing. Create AWS CloudFormation templates to launch the application by using EC2 user data to install and configure the application.

C. Run a website as an AWS Elastic Beanstalk application, storing the images in Amazon S3, and using an Amazon RDS database for user accounts and sharing. Create AWS CloudFormation templates to launch the application and perform blue/green deployments.

D. Run a website from an Amazon S3 bucket that authorizes Amazon AppStream to stream applications for a combined image viewer and messenger that stores images in Amazon S3.
Have the website use an Amazon RDS database for user accounts and sharing.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Messaging data in s3 is a bad idea. Cognito cannot handle sharing very well

**QUESTION 135**
A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda and Amazon DynamoDB. They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept Amazon CloudWatch metrics did not indicate any issues with DynamoDB but showed that some Lambda functions were hitting their timeout.
Which of the following actions should the Solutions Architect consider to improve performance? (Choose two.)

A. Configure the AWS Lambda function to reuse containers to avoid unnecessary startup time.

B. Increase the amount of memory and adjust the timeout on the Lambda function.
Complete performance testing to identify the ideal memory and timeout configuration for the Lambda function.

C. Create an Amazon ElastiCache cluster running Memcached, and configure the Lambda function for VPC integration with access to the Amazon ElastiCache cluster.

D. Enable API cache on the appropriate stage in Amazon API Gateway, and override the TTL for individual methods that require a lower TTL than the entire stage.

E. Increase the amount of CPU, and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal CPU and timeout configuration for the Lambda function.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
You cannot increase CPU for lambda. CPU is related to memory
https://docs.aws.amazon.com/lambda/latest/dg/resource-model.html

**QUESTION 136**
A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:
- The data must be highly durable and available.
- The data must always be encrypted at rest and in transit.
- The encryption key must be managed by the company and rotated periodically. Which of the following solutions should the Solutions Architect recommend?

A. Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
B. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.
C. Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.
D. Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.File gateway link to S3, need to encrypt S3 as well
D.You may not be able to rotate the key



**QUESTION 137**
A Solutions Architect is designing a highly available and reliable solution for a cluster of Amazon EC2 instances.
The Solutions Architect must ensure that any EC2 instance within the cluster recovers automatically aftert a system failure. The solution must ensure that the recovered instance maintains the same IP address.
How can these requirements be met?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Private IP could change
D.StatusCheckFailed_System is for system wise problem, and this is what the question is asking for
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html#types-of-instance-status-checks

**QUESTION 138**

A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check. Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times. Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (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.

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.Full stack health check on Route 53 level can reduce the number of requests a lot as we don't need to check each instance
C.Target group health check for ALB need to be HTTP or HTTPS. For TCP you will need a NLB
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html

**QUESTION 139**
A company is running an email application across multiple AWS Regions. The company uses Ohio (us-east-2) as the primary Region and Northern Virginia (us-east-1) as the Disaster Recovery (DR) Region. The data is continuously replicated from the primary Region to the DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time, but it affects the application's RPO. Which of the following solutions should help remediate this performance problem? (Select TWO)

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

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.This could be a good solution as it enables scaling on both side

**QUESTION 140**
A company has implemented AWS Organizations. It has recently set up a number of new accounts and wants to deny access to a specific set of AWS services in these new accounts.
How can this be controlled MOST efficiently?

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 141**
A company is planning to migrate an application from on-premises to AWS. The application currently uses an Oracle database and the company can tolerate a brief downtime of 1 hour when performing the switch to the new infrastructure. As part of the migration, the database engine will be changed to MySQL. A Solutions Architect needs to determine which AWS services can be used to perform the migration while minimizing the amount of work and time required.
Which of the following will meet the requirements?

A. Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to analyse the current schema and provide a recommendation for the optimal database engine. Then, use AWS DMS to migrate to the recommended enginer.
Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.
B. Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to begin moving data from the on-premises database to AWS.
After the initial copy, continue to use AWS DMS to keep the databases insync until cutting over to the new database. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.
C. Use AWS DMS to help identify the best target deployment between installing the database engine on Amazon EC2 dierctly or moving to Amazon RDS. Then, use AWS DMS to migrate to the platform. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.
D. Use AWS DMS to begin moving data from the on-premises database to AWS. After the intitial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.By default the engine will always be innodb
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.MySQL.html
B.https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/CHAP_Converting.App.html
https://aws.amazon.com/dms/faqs/
C.Application Discovery service is just not used for this….

**QUESTION 142**
A Solutions Architect has created an AWS CloudFormation template for a three-tier application that contains an Auto Scaling group of Amazon EC2 instances running a custom AMI.
The Solutions Architect wants to ensure that future updates to the custom AMI can be deployed to a running stack by first updating the template to refer to the new AMI, and then invoking UpdateStack to replace the EC2 instances with instances launched from the new AMI.
How can updates to the AMI be deployed to meet these requirements?

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 to Replace. DeletionPolicy
C. Edit the AWS::AutoScaling: :AutoScalingGroup resource in the template, inserting an attribute. UpdatePolicy
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.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 143**
Your company has a logging microservice which is used to generate logs when users have entered certain commands in another application. This logging service is implemented via an SQS standard queue that an EC2 instance is listening to. However, you have found that on some occasions, the order of the logs are not maintained. As a result, it becomes harder to use this
service to trace users' activities. How should you fix this issue in a simple way?

A. Convert the existing standard queue into a FIFO queue. Add a deduplication ID for the messages that are sent to the queue.
B. Delete the existing standard queue and recreate it as a FIFO queue. As a result, the order for the messages to be received is ensured.
C. Migrate the whole microservice application to SWF so that the operation sequence is guaranteed.
D. The wrong order of timestamps is a limitation of SQS, which does not have a fix.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
A.Can't do this
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html#FIFO-queues-moving



**QUESTION 144**
A large trading company is using an on-premise system to analyze the trade data. After the trading day closes, the data including the day's transaction costs, execution reporting, and market performance is sent to a Redhat server which runs big data analytics tools for predictions for next day trading. A bash script is used to configure resource and schedule when to run the data analytics workloads. How should the on-premise system be migrated to AWS with appropriate tools? (Select THREE)

A. Create a S3 bucket to store the trade data that is used for post processing.
B. Send the trade data from various sources to a dedicated SQS queue.
C. Use AWS Batch to execute the bash script using a proper job definition.
D. Create EC2 instances with auto-scaling to handle with the big data analytics workloads.
E. Use CloudWatch Events to schedule the data analytics jobs.

**Correct Answer:** ACD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 145**
A large IT company has an on-premise website which provides real-estate information such as renting, house prices and latest news to users. The website has a Java backend and a NoSQL MongoDB database that is used to store subscribers data. You are a cloud analyst and need to migrate the whole application to AWS platform. Your manager requires that a similar structure should be deployed in AWS for high availability. Moreover, a tracing framework is essential which can record data from both the client request and the downstream call to the database in AWS. Which AWS services should you choose to implement the migration? Select 3 Options.

A. Deploy an autoscaling group of Java backend servers to provide high availability
B. Use RDS Aurora as the database for the subscriber data because it is highly available and can scale up to 15 Read Replicas.
C. Create a DynamoDB database to hold subscriber data. Set up an autoscaling policy for the read/write throughput.
D. Use AWS X-Ray SDK to record data about incoming and outgoing requests. View the statistics graph in X-Ray console.
E. Trace the requests using AWS JAVA SDK and send logs to AWS CloudWatch Events. Create a CloudWatch dashboard to view the statistics.

**Correct Answer:** ACD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 146**
You work in a video game company and your team is working on a feature that tells how many times that certain web pages have been viewed or clicked. You also created an AWS Lambda function to show some key statistics of the data. You tested the Lambda function and it worked perfectly.
However, your team lead requires you to show the statistics every day at 8:00AM GMT on a big TV screen so that when employees come in to the office every morning, they have a rough idea of how the feature runs. What is the most cost efficient and straightforward way for you to make this happen?

A. Create an AWS CloudWatch Events rule that is scheduled using a cron expression as ?0 08 * * ? *? Configure the target as the Lambda function.
B. Create an Amazon linux EC2 T2 instance and set up a Cron job using Crontab. Use AWS CLI to call your AWS Lambda every 8:00AM.
C. Use Amazon Batch to set up a job with a job definition that runs every 8:00AM for the Lambda function.
D. In AWS CloudWatch Events console, click reate Event?using the cron expression ?* ? * * 08 00? Configure the target as the Lambda function.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
This will run every year on  Aug?
Not sure here as Cron expression is not clear. Could be C here

**QUESTION 147**
A supermarket chain had a big data analysis system deployed in AWS. The system has the raw data such as clickstream or process logs in S3. A m3.large EC2 instance transformed the data to other formats and saved it to another S3 bucket. Amazon Redshift analysed the data afterwards.
Your team is in charge of improving the system using AWS Glue which is a fully managed ETL (extract, transform, and load) service. Which tasks can AWS Glue simplify during re-establishing the big data system? (Select TWO)

A. AWS Glue contains a crawler that connects to the S3 bucket and scans the dataset. Then the service creates metadata tables in the data catalog.

B. AWS Glue automatically generates code in Java to extract data from the source and transform the data to match the target schema.
C. Be default, AWS Glue creates a scheduler to trigger the activated tasks every minute.
D. AWS Glue has a central metadata repository (data catalog). The data in the catalog is available for analysis immediately.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 148**
An AWS Solutions Architect has noticed that their company is using almost exclusively EBS General Purpose SSD (gp2) volume types for their EBS volumes. They are considering modifying the type of some of these volumes, but it is important that performance is not affected. Which of the following actions could the Solutions Architect consider? (Select TWO)

A. A 50GB gp2 root volume can be modified to an EBS Provisioned IOPS SSD (io1) without stopping the instance.
B. A gp2 volume that is attached to an instance as a root volume needs can be modified to a Throughput Optimized HDD (st1) volume.
C. A 1GB gp2 volume that is attached to an instance as a non-root volume can be modified to a Cold HDD (sc1) volume.
D. A 1TB gp2 volume that is attached to an instance as a non-root volume can be modified to a Throughput Optimized HDD (st1) volume without stopping the instance or detaching the volume.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.This cannot happen
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/modify-volume-requirements.html
C.Won't work as SC1 has min size 500gb
https://aws.amazon.com/ebs/features/
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/modify-volume-requirements.html

**QUESTION 149**
Which of the following are associated with using the "HLS" method of viewing the Kinesis video stream? (Select TWO)

A. A web application that is able to display the video stream using the third-party player Video.js.
B. In order to process Kinesis video streams, a SAAS provider needs to build a new video player which is integrated into their major online product.
C. Able to view only live video, not archived video.
D. Playback video by typing in the HLS streaming session URL in the location bar of the Apple Safari browser for debug purpose.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
B.You don't need a player to process video streams
C.Can work with both live and on demand video
https://aws.amazon.com/blogs/aws/amazon-kinesis-video-streams-adds-support-for-hls-output-streams/
D.It can be used with a browser
https://docs.aws.amazon.com/kinesisvideostreams/latest/dg/

API_reader_GetHLSStreamingSessionURL.html

**QUESTION 150**
A team has just received a task to build an application that needs to recognize faces in streaming videos. They will get the source videos from a third party which use a container format (MKV). The APP should be able to quickly address faces through the video in real time and save the output in a suitable manner for downstream to process. As recommended by the AWS Solutions Architect colleague, they would like to develop the service using AWS Rekognition. Which below options are needed to accomplish the task? Select 3.

A. S3 buckets to store the source MKV videos for AWS Rekognition to process. S3 should be used in this case as it has provided an unlimited, highly available and durable storing space.
Make sure that the third party has the write access to S3 buckets.
B. A Kinesis video stream for sending streaming video to Amazon Rekognition Video. This can be done by using Kinesis utMedia?API in Java SDK. The PutMedia operation writes video data fragments into a Kinesis video stream that Amazon Rekognition Video consumes.
C. An Amazon Rekognition Video stream processor to manage the analysis of the streaming video. It can be used to start, stop, and manage stream processors according to needs.
D. Use EC2 or Lambda to call Rekognition API etectFaces?with the source videos saved in S3 bucket. For each face detected, the operation returns face details. These details include a bounding box of the face, a confidence value, and a fixed set of attributes such as facial landmarks, etc.
E. After the APP has utilized Rekognition API to fetch the recognized faces from live videos, use S3 or RDS database to store the output from Rekognition. Another lambda can be used to post-process the result and present to UI.
F. A Kinesis data stream consumer to read the analysis results that Amazon Rekognition Video sends to the Kinesis data stream. It can be an Amazon EC2 instance by adding to one of Amazon Machine Images (AMIs). The consumer can be autoscaled by running it on multiple Amazon EC2 instances under an Auto Scaling group.

**Correct Answer:** BCF
**Section: (none)**
**Explanation**

**Explanation/Reference:**
https://docs.aws.amazon.com/rekognition/latest/dg/streaming-video.html



**QUESTION 151**
A large company starts to use AWS organizations with consolidated billing feature to manage its separate departments. The AWS operation team has just created 3 OUs (organization units) with 2 AWS accounts each. To be compliant with company-wide security policy, CloudTrail is required for all AWS accounts which is already been set up. However after some time, there are cases that users in certain OU have turned off the CloudTrail of their accounts. What is the best way for the AWS operation team to prevent this from happening again?

A. Update the AWS Organizations feature sets to features?and then create a Service Control Policies (SCP) to Prevent Users from Disabling AWS CloudTrail. This can be achieved by a deny policy with cloudtrail:StopLogging denied.
B. This can be achieved by Service Control Policies (SCP) in features?set. The team needs to delete and recreate the AWS Organizations with features?enabled and then use a proper control policy to limit the operation of cloudtrail:StopLogging.
C. In each AWS account in this organization, create an IAM policy to deny cloudtrail:StopLogging for all users including administrators.
D. Use a Service Control Policies (SCP) to prevent users from disabling AWS CloudTrail. This can be done by a allow policy which denies cloudtrail:StopLogging

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Organisation do not need to be recreated to enable all features set.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html

**QUESTION 152**
A mobile App developer just made an App in both IOS and Android that has a feature to count step numbers. He has used AWS Cognito to authorize users with a user pool and identity pool to provide access to AWS DynamoDB table. The App uses the DynamoDB table to store user subscriber data and number of steps. Now the developer also needs Cognito to integrate with Google to provide federated authentication for the mobile application users so that user does not need to remember extra login access.What should the developer do to make this happen for the IOS and Android App?

A. Amazon Cognito Identity pools (federated identities) support user authentication through federated identity providers-including Amazon, Facebook, Google, and SAML identity providers. The developer just needs to set up the federated identities for Google access
B. Only Android works for federated identities if Google access is required for AWS Cognito. This can be done by configuring Cognito identity pools with a Google Client ID.
C. Amazon Cognito User pools support user authentication through federated identity providersincluding Amazon, Facebook, Google, and SAML identity providers. The developer just needs to set up the federated identities for Google access in Cognito User pool.
D. Only IOS (Objective-C and Swift) works for federated identities if Google access is required for AWS Cognito. This can be done by configuration Cognito identity pools with a Google Client ID. Google federated access does not work for android app.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
User pool cannot authorise access for AWS resource. You will need an identity pool. User pool is just a user directory.
https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-identity.html

**QUESTION 153**
A big company has a service to process gigantic clickstream data sets which are often the result of holiday shopping traffic on a retail website, or sudden dramatic growth on the data network of a media or social networking site. It is becoming more and more expensive to analyze these clickstream datasets for its on-premise infrastructure. As the sample data set keeps growing, fewer applications are available to provide a timely response. The service is using a Hadoop cluster with Cascading. How can they migrate the applications to AWS in the best way?

A. Put the source data to S3 and migrate the processing service to an AWS EMR hadoop cluster with Cascading. Enable EMR to directly read and query data from S3 buckets. Write the output to RDS database
B. Put the source data to a Kinesis stream and migrate the processing service to AWS lambda to utilize its scaling feature. Enable lambda to directly read and query data from Kinesis stream. Write the output to RDS database
C. Put the source data to a S3 bucket and migrate the processing service to AWS EC2 with auto scaling. Ensure that the auto scaling configuration has proper maximum and minimum number of instances. Monitor the performance in Cloudwatch dashboard. Write the output to DynamoDB table for downstream to process.
D. Put the source data to a Kinesis stream and migrate the processing service to an AWS EMR cluster with Cascading. Enable EMR to directly read and query data from Kinesis streams. Write the output to Redshift.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
For large dataset, it makes sense to use kinesis with EMR. If we just store the dataset in S3, it makes not much differences than the on prem solution.

**QUESTION 154**
An Artificial Intelligence startup company has used lots of EC2 instances. Some instances use SQL Server

database while the others use Oracle. As the data needs to be kept secure, regular snapshots are required. They want SQL Server EBS volume to take snapshot every 12 hours.
However for Oracle, it only needs a snapshot every day. Which option below is the best one that the company should choose without extra charge?

A. Use free third-party tool such as Clive to Manage EC2 instance lifecycle. It can design various backup policies for EC2 EBS volumes. Add a 12 hours backup policy to SQL Server EBS volumes and a 24 hours backup policy to Oracle EBS volumes.
B. Add a prefix to the name of both SQL Server and Oracle EBS volumes. In AWS Data Lifecycle Management console, create two management policies based on the name prefix.
For example, add a 12 hours backup schedule to EBS volumes with a name starting with sql and add a 24 hours backup schedule to EBS volumes with a name starting with oracle?
C. Create a dedicate Lambda function to differentiate EC2 EBS volumes and take snapshots.
Set up Cloudwatch Events Rules to call the lambda so that the function runs every 12 hours for SQL Server and 24 hours for Oracle.
D. Add different tags for SQL Server and Oracle EBS volumes. In AWS Data Lifecycle Management console, create two management policies based on the tags. Add a 12 hours schedule to SQL Server lifecycle policy and a 24 hours schedule to Oracle lifecycle policy

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 155**
API gateway and Lambda non-proxy integrations have been chosen to implement an application by a software engineer. The application is a data analysis tool that returns some statistic results when the HTTP endpoint is called. The lambda needs to communicate with some back-end data services such as Keen.io however there are chances that error happens such as wrong data requested, bad communications, etc. The lambda is written using Java and two exceptions may be returned which are BadRequestException and InternalErrorException. What should the software engineer do to map these two exceptions in API gateway with proper HTTP return codes? For example, BadRequestException and InternalErrorException are mapped to HTTP return codes 400 and 500 respectively. Select 2.

A. Add the corresponding error codes (400 and 500) on the Integration Response in API gateway
B. Add the corresponding error codes (400 and 500) on the Method Response in API gateway.
C. Put the mapping logic into Lambda itself so that when exception happens, error codes are returned at the same time in a JSON body.
D. Add Integration Responses where regular expression patterns are set such as BadRequest or InternalError. Associate them with HTTP status codes
E. Add Method Responses where regular expression patterns are set such as BadRequest or InternalError. Associate them with HTTP status codes 400 and 500.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-method-settings-method-response.html
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-integration-settings-integration-response.html

**QUESTION 156**
An IT company owns a web product in AWS that provides discount restaurant information to customers. It has used one S3 Bucket (my_bucket) to store restaurant data such as pictures, menus, etc. The product is deployed in VPC subnets. The company's Cloud Architect decides to configure a VPC endpoint for this S3 bucket so that the performance will be enhanced. To be compliance to security rules, it is required that the new VPC endpoint is only used to communicate with this specific S3 Bucket and on the other hand, the S3 bucket only allows the read/write operations coming from this VPC endpoint. Which two options should the

Cloud Architect choose to meet the security needs?

A. Use a VPC Endpoint policy for Amazon S3 to restrict access to the S3 Bucket "my_bucket" so that the VPC Endpoint is only allowed to perform S3 actions on "my_bucket".
B. Modify the security group of the EC2 instance to limit the outbound actions to the VPC Endpoint if the outgoing traffic destination is the S3 bucket "my_bucket"".
C. In the S3 bucket "my_bucket", add a S3 bucket policy in which all actions are denied if the source IP address is not equal to the EC2 public IP (use "NotIpAddress" condition).
D. For the S3 bucket "my_bucket", use a S3 bucket policy that denies all actions if the source VPC Endpoint is no equal to the endpoint ID that is created.s
E. Create a S3 bucket policy in the S3 bucket "my_bucket" which denies all actions unless the source IP address is equal to the EC2 public IP (use "IpAddress" condition).

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 157**
You work for an e-commerce retailer as an AWS Solutions Architect. Your company is looking to improve customer loyalty programs by partnering with other third-parties to offer a more comprehensive selection of customer rewards. You plan to use Amazon Managed Blockchain to implement a blockchain network that allows your company and third-parties to share and validate rewards information quickly and transparently. How do you add members for this blockchain?

A. When Amazon Managed Blockchain is set up, there is an initial member in the AWS account. Then new members can be added in this AWS account without having to send an invitation, or a network invitation can be created for a member in a different AWS account
B. While Amazon Managed Blockchain is configured, there is an initial member in the AWS account. Then new members can be added in this AWS account without having to send an invitation. You cannot add new members for other AWS accounts
C. When Amazon Managed Blockchain is created, there is no any member in the AWS account. Then new members can be added in this AWS account or other accounts by sending out an an invitation.
D. When Amazon Managed Blockchain is firstly created, there is no any member in the AWS account. Then new members can be added in this AWS account. For other accounts, they can join this net blockchain network by using the network ID.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
https://docs.aws.amazon.com/managed-blockchain/latest/managementguide/get-started-create-network.html

**QUESTION 158**
A company has deployed an application to multiple environments in AWS, including production and testing. The company has separate accounts for production and testing, and users are allowed to create additional application users for team members or services, as needed. The Security team has asked the Operations team for better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments.

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

A. Create a new AWS account to hold user and service accounts, such as an identity account. Create users and groups in the identity account. Create roles with appropriate permissions in the production and testing accounts. Add the identity account to the trust policies for the roles.
B. Modify permissions in the production and testing accounts to limit creating new IAM users to members of the Operations team. Set a strong IAM password policy on each account. Create new IAM users and

groups in each account to limit developer access to just the services required to complete their job function.

C. Create a script that runs on each account that checks user accounts for adherence to a security policy. Disable any user or service accounts that do not comply.

D. Create all user accounts in the production account. Create roles for access in the production account and testing accounts. Grant cross-account access from the production account to the testing account.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 159**
The CISO of a large enterprise with multiple IT departments, each with its own AWS account, wants one central place where AWS permissions for users can be managed and users authentication credentials can be synchronized with the company's existing on-premises solution.

Which solution will meet the CISO's requirements?

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 de provision accounts based on data in the on-premises solution.



**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
2019-10-19

**QUESTION 160**
A large company has increased its utilization of AWS over time in an unmanaged way. As such, they have a large number of independent AWS accounts across different business units, projects, and environments. The company has created a Cloud Center of Excellence team, which is responsible for managing all aspects of the AWS Cloud, including their AWS accounts.

Which of the following should the Cloud Center of Excellence team do to BEST address their requirements in a centralized way? (Select rwo.)

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.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 161**
To abide by industry regulations, a Solutions Architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The Solutions Architect is required to provide access to the data stored in AWS to the company's global WAN network. The Security team mandates that no traffic accessing this data should traverse the public internet.

How should the Solutions Architect design a highly available solution that meets the requirements and is cost-effective?

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.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 162**
A company wants to manage the costs associated with a group of 20 applications that are critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology. Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often for several hours.

Which is the MOST cost-effective solution?

A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.
B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch.
C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have

sufficient resources. Monitor each AWS Elastic Beanstalk deployment with using CloudWatch alarms.

D. Deploy a new amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 163**
A Solutions Architect must build a highly available infrastructure for a popular global video game that runs on a mobile phone platform. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The database tier is an Amazon RDS MySQL. Multi-AZ instance. The entire application stack is deployed in both us-east-1 and eu-central-1. Amazon Route 53 is used to route traffic to the two installations using a latency-based routing policy. A weighted routing policy is configured in Route 53 as a fail over to another region in case the installation in a region becomes unresponsive.

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

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

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

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 164**
An online e-commerce business is running a workload on AWS. The application architecture includes a web tier, an application tier for business logic, and a database tier for user and transactional data management. The database server has a 100 GB memory requirement. The business requires cost-efficient disaster recovery for the application with an RTO of 5 minutes and an RPO of 1 hour. The business also has a regulatory for out-of region disaster recovery with a minimum distance between the primary and alternate sites of 250 miles.

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

A. Back up the application and database data frequently and copy them to Amazon S3. Replicate the backups using S3 cross-region replication, and use AWS CloudFormation to instantiate infrastructure for disaster recovery and restore data from Amazon S3.
B. Employ a pilot light environment in which the primary database is configured with mirroring to build a standby database on m4.large in the alternate region. Use AWS CloudFormation to instantiate the web servers, application servers and load balancers in case of a disaster to bring the application up in the

alternate region. Vertically resize the database to meet the full production demands, and use Amazon Route 53 to switch traffic to the alternate region.

C. Use a scaled-down version of the fully functional production environment in the alternate region that includes one instance of the web server, one instance of the application server, and a replicated instance of the database server in standby mode. Place the web and the application tiers in an Auto Scaling behind a load balancer, which can automatically scale when the load arrives to the application. Use Amazon Route 53 to switch traffic to the alternate region.

D. Employ a multi-region solution with fully functional web, application, and database tiers in both regions with equivalent capacity. Activate the primary database in one region only and the standby database ir the other region. Use Amazon Route 53 to automatically switch traffic from one region to another using health check routing policies.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 165**
A company runs a memory-intensive analytics application using on-demand Amazon EC2 compute optimized instance. The application is used continuously and application demand doubles during working hours. The application currently scales based on CPU usage. When scaling in occurs, a lifecycle hook is used because the instance requires 4 minutes to clean the application state before terminating.

Because users reported poor performance during working hours, scheduled scaling actions were implemented so additional instances would be added during working hours. The Solutions Architect has been asked to reduce the cost of the application.

Which solution is MOST cost-effective?

A. Use the existing launch configuration that uses C5 instances, and update the application AMI to include the Amazon CloudWatch agent. Change the Auto Scaling policies to scale based on memory utilization. Use Reserved Instances for the number of instances required after working hours, and use Spot Instances to cover the increased demand during working hours.

B. Update the existing launch configuration to use R5 instances, and update the application AMI to include SSM Agent. Change the Auto Scaling policies to scale based on memory utilization. Use Reserved instances for the number of instances required after working hours, and use Spot Instances with on-Demand instances to cover the increased demand during working hours.

C. Use the existing launch configuration that uses C5 instances, and update the application AMI to include SSM Agent. Leave the Auto Scaling policies to scale based on CPU utilization. Use scheduled Reserved Instances for the number of instances required after working hours, and use Spot Instances to cover the increased demand during work hours.

D. Create a new launch configuration using R5 instances, and update the application AMI to include the Amazon CloudWatch agent. Change the Auto Scaling policies to scale based on memory utilization. use Reserved Instances for the number of instances required after working hours, and use Standard Reserved Instances with On-Demand Instances to cover the increased demand during working hours.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 166**
A company has a data center that must be migrated to AWS as quickly as possible. The data center has a 500 Mbps AWS Direct Connect link and a separate, fully available 1 Gbps ISP connection. A Solutions Architect must transfer 20 TB of data from the data center to an Amazon S3 bucket.

What is the FASTEST way transfer the data?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 167**
A company wants to follow its website on AWS using serverless architecture design patterns for global customers. The company has outlined its requirements as follow:
- The website should be responsive.
- The website should offer minimal latency.
- The website should be highly available.
- Users should be able to authenticate through social identity providers such as Google, Facebook, and Amazon.
- There should be baseline DDoS protections for spikes in traffic.

How can the design requirements be met?

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



**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 168**
A company is currently using AWS CodeCommit for its source control and AWS CodePipeline for continuous integration. The pipeline has a build stage for building the artifacts which is then staged in an Amazon S3 bucket.

The company has identified various improvement opportunities in the existing process, and a Solutions Architect has been given the following requirement:

- Create a new pipeline to support feature development
- Support feature development without impacting production applications
- Incorporate continuous testing with unit tests
- Isolate development and production artifacts
- Support the capability to merge tested code into production code.

How should the Solutions Architect achieve these requirements?

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.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 169**
A company runs an ordering system on AWS using Amazon SQS and AWS Lambda, with each order received as a JSON message. recently the company had a marketing event that led to a tenfold increase in orders. With this increase, the following undesired behaviors started in the ordering system:

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

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

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

How should the Solutions Architect meet these requirements?

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

B. Receive single messages with each Lambda invocation, put additional Lambda workers to poll the queue, delete messages after processing, increase the message timer for the messages, use Amazon CloudWatch Logs for messages that could not be processed, create a CloudWatch alarm on Lambda errors for notification.

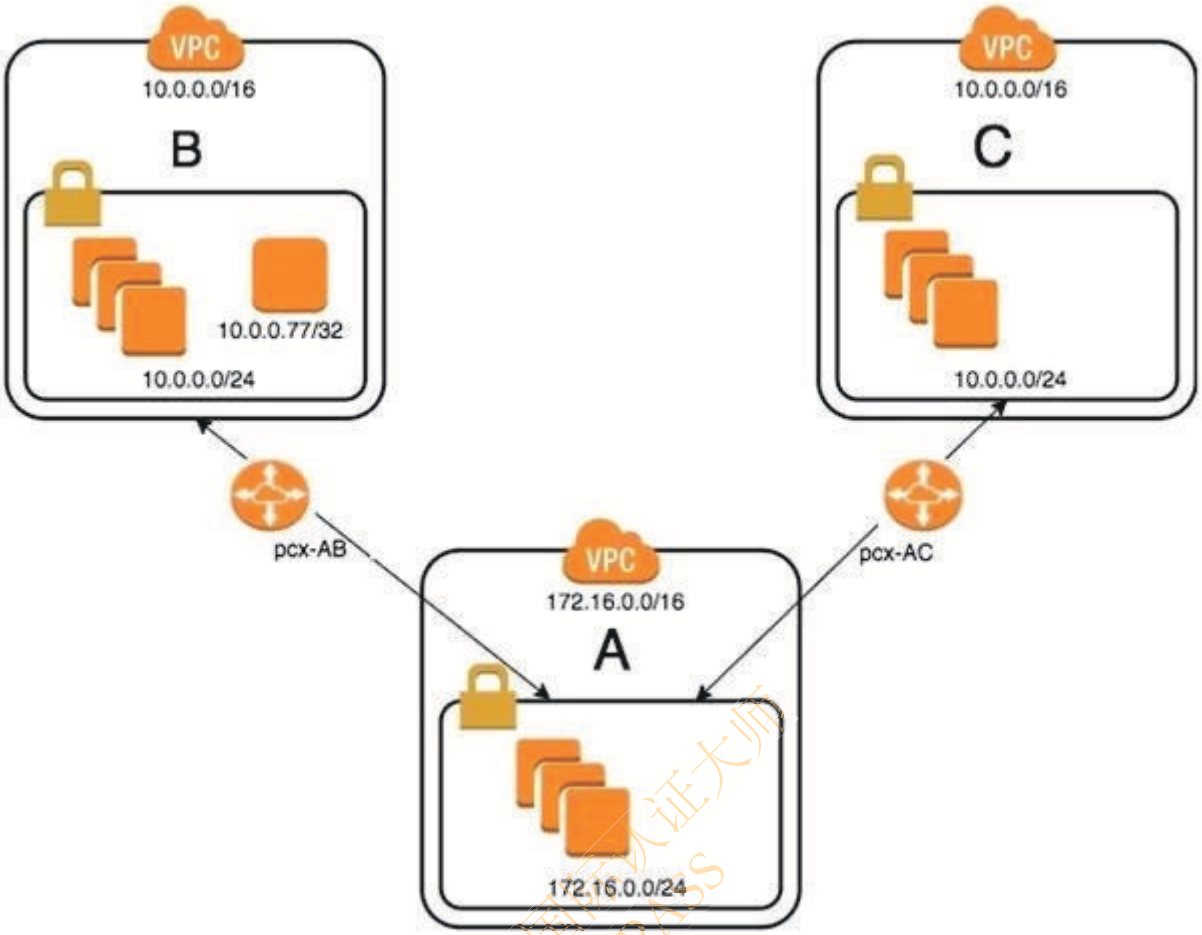
C. Receive multiple messages with each Lambda invocation, use long polling when receiving the messages, log the errors from the message processing code using Amazon CloudWatch Logs, create a dead letter queue with AWS Lambda to capture failed invocations, create CloudWatch events on Lambda errors for notification.

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 170**
An organization has recently grown through acquisitions. Two of the purchased companies use the same IP CIDR range. There is a new short-term requirement to allow AnyCompany A (VPC- A) to communicate with a server that has the IP address 10.0.0.77 in AnyCompany B (VPC-B). AnyCompany A must also communicate with all resources in AnyCompany C (VPC-C). The Network team has created the VPC peer links, but it is having issues with communications between VPC-A and VPC-B. After an investigation, the team believes that the routing tables in the VPCs are incorrect.




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

A. On VPC-A, create a static route for the VPC-B CIDR range (10.0.0.0/24) across VPC peer pcx-AB. Create a static route of 10.0.0.0/16 across VPC peer pcx-AC.
On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) on peer pcx-AB.
On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.

B. On VPC-A, enable dynamic route propagation on pcx-AB and pcx-AC.
On VPC-B, enable dynamic route propagation and use security groups to allow only the IP address 10.0.0.77/32 on VPC peer pcx-AB.
On VPC-C, enable dynamic route propagation with VPC-A on peer pcx-AC.

C. On VPC-A, create network access control lists that block the IP address 10.0.0.77/32 on VPC peer pcx-AC.
On VPC-A, create a static route for VPC-B CIDR (10.0.0.0/24) on pcx-AB and a static route for VPC-C CIDR (10.0.0.0/24) on pcx-AC.
On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AB.
On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.

D. On VPC-A, create a static route for the VPC-B CIDR (10.0.0.77/32) 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.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 171**
A company is designing a new highly available web application on AWS. The application requires consistent and reliable connectivity from the application servers in AWS to a backend REST API hosted in the company's on-premises environment. The backend connection between AWS and on-premises will be routed over an AWS Direct Connect connection through a private virtual interface. Amazon Route 53 will be used to manage private DNS records for the application to resolve the IP address on the backend REST API.

Which design would provide a reliable 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.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 172**
A retail company is running an application that stores invoice files in Amazon S3 bucket and metadata about the files in an Amazon. The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region.

Which option meets these requirements?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 173**
A company wants to launch an online shopping website in multiple countries and must ensure that customers are protected against potential "man-in-the-middle" attacks.

Which architecture will provide the MOST secure site access?

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

B. Register 2048-bit encryption keys from a third-party certificate service. Use a third-party DNS provider that uses the customer managed keys for DNSSec. Upload the keys to ACM, and use ACM to automatically deploy the certificates for secure web services to an EC2 front-end web server fleet by using NGINX. Use the Server Name Identification extension in all client requests to the site.

C. Use Route 53 for domain registration. Register 2048-bit encryption keys from a third-party certificate. Use a third-party DNS service that supports DNSSEC for DNS requests that use the customer managed keys. Import the customer managed keys to ACM to deploy the certificates to Classic Load Balancers configured with those TLS/SSL certificates for the site. Use the Server Name Identification extension in all clients requests to the site.

D. Use Route 53 for domain registration, and host the company DNS root servers on Amazon EC2 instances running Bind. Enable DNSSEC for DNS requests. Use ACM to register TLS/SSL certificates for the shopping website, and use Application Load Balancers configured with those TLS/ SSL certificates for the site. Use the Server Name Identification extension in all client requests to the site.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 174**
A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle or least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes.

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

A. Create a new AWS Organizations account. Create groups in Active Directory and assign them to roles in AWS to grant federated access. Require each team to tag their resources, and separate bills based on tags. Control access to resources through IAM granting the minimally required privilege.

B. Create individual accounts for each team. Assign the security 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 to provide the Finance team with the resource use for each team based on tagging. Isolate resources using IAM to avoid account sprawl. Security will control and monitor logs and permissions.

D. Create a master account for billing using Organizations, and create each team's account from that master account. Create a security account for logs and cross-account access. Apply service control policies on each account, and grant the Security team cross-account access to all accounts. Security will create IAM policies for each account to maintain least privilege access.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 175**
A company has a 24 TB MySQL database in its on-premises data center that grows at the rate of 10 GB per day. The data center is connected to the company's AWS infrastructure with a 50 Mbps VPN connection.

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

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

A. 1. Use the VM Import/Export service to import a snapshot on the on-premises database into AWS.
2. Launch a new EC2 instance from the snapshot.
3. Set up ongoing database replication from on premises to the EC2 database over the VPN.
4. Change the DNS entry to point to the EC2 database.
5. Stop the replication.

B. 1. Launch an AWS DMS instance.
2. Launch an Amazon RDS Aurora MySQL DB instance.
3. Configure the AWS DMS instance with on-premises and Amazon RDS database information.
4. Start the replication task within AWS DMS over the VPN.
5. Change the DNS entry to point to the Amazon RDS MySQL database.
6. Stop the replication.

C. 1. Create a database export locally using database-native tools.
2. Import that into AWS using AWS Snowball.
3. Launch an Amazon RDS Aurora DB instance.
4. Load the data in the RDS Aurora DB instance from the export.
5. Set up database replication from the on-premises database to the RDS Aurora DB instance over the VPN.
6. Change the DNS entry to point to the RDS Aurora DB instance.
7. Stop the replication.

D. 1. Take the on-premises application offline.
2. Create a database export locally using database-native tools.
3. Import that into AWS using AWS Snowball.
4. Launch an Amazon RDS Aurora DB instance.
5. Load the data in the RDS Aurora DB instance from the export.
6. Change the DNS entry to point to the Amazon RDS Aurora DB instance.
7. Put the Amazon EC2 hosted application online.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**



**QUESTION 176**
A company wants to allow its Marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The Team Manager must have the ability to manage users and groups, but no team members should have access to services or resources not required for the SQL queries. Additionally, Administrators need to audit the queries made and receive notifications when a query violates rules defined by the Security team.

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

Which design meets these requirements?

A. Apply a service control policy (SCP) that allows access to IAM, Amazon RDS, and AWS CloudTrail. Load customer records in Amazon RDS MySQL and train users to execute queries using the AWS CLI. Stream the query logs to Amazon CloudWatch Logs from the RDS database instance. use a subscription filter with AWS lambda functions to audit and alarm on queries against personal data.

B. Apply a service control policy (SCP) that denies access to all services except IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer record files in Amazon S3 and train users to execute queries using the CLI via Athena. Analyze CloudTrail events to audit and alarm on queries against personal data.

C. Apply a service control policy (SCP) that denies to all services except IAM, Amazon DynamoDB, and AWS CloudTrail. Store customer records in DynamoDB and train users to execute queries using the AWS CLI. Enable DynamoDB streams to track the queries that are issued and use an AWS Lambda function for real-time monitoring and alerting.

D. Apply a service control policy (SCP) that allows to IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer records as files in Amazon S3 and train users to leverage the Amazon S3 Select feature and execute queries using the AWS CLI. Enable S3 object-level logging and analyze

CloudTrail events to audit and alarm on queries against personal data.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 177**
A Solutions Architect is responsible for redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high- memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds them to an in-memory queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them, and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average., most of which is spent waiting on external service calls, but the application is written to process multiple items in parallel.

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

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

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

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 178**
A Solutions Architect needs to migrate a legacy application from on premises to AWS. On premises, the application runs on two Linux servers behind a load balancer and accesses a database that is master-master on two servers. Each application server requires a license file that is tied to the MAC address of the server's network adapter. It takes the software vendor 12 hours to send ne license files through email. The application requires configuration files to use static. IPv4 addresses to access the database servers, not DNS.

Given these requirements, which steps should be taken together to enable a scalable architecture for the

application servers? (Choose 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.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 179**

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

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

What CI/CD configuration meets all of the requirements?

A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update.

B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.

C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update.

D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.

A. A
B. B
C. C
D. D

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**