You have just set up a Service Catalog portfolio and collection of products for your users. Unfortunately, the users are having difficulty launching one of the products and are getting "access denied" messages. What could be the cause of this?

1. The product does not have a launch constraint assigned.
2. The template constraint assigned to the product does not have the proper permissions.
3. The user launching the product does not have required permissions to launch the product.
4. A Service Catalog Policy has not yet been applied to the account.
5. The launch constraint does not have permissions to CloudFormation.
6. The notification constraint did not have access to the S3 location for the product's CloudFront template.

Answer: a, c, e

EXPLANATION:

For Service Catalog products to be successfully launched, either a launch constraint must be assigned and have sufficient permission to deploy the product or the user must have the same required permissions.

On your last Security Penetration Test Audit, the auditors noticed that you were not effectively protecting against SQL injection attacks. Even though you don't have any resources that are vulnerable to that type of attack, your Chief Information Security Officer insists you do something. Your organization consists of approximately 30 AWS accounts. Which steps will allow you to most efficiently protect against SQL injection attacks?

1. Create a custom NACL filter using Lambda@Edge to check requests for SQL code. Use OpsWorks to apply the NACL across all public subnets across the organization.
2. Use AWS WAF to create an ACL that denies requests that include SQL code. Assign the ACL to Firewall Manager instances in each account using AWS OpsWorks.
3. Ensure all sub-accounts are members of an organization in the AWS Organizations service and use Consolidated Billing. Subscribe to AWS Shield Advanced to automatically enable SQL injection protection across all sub-accounts.
4. Ensure all sub-accounts are members of an organization in the AWS Organizations service. Use Firewall Manager to create an ACL rule to deny requests that contain SQL code. Apply the ACL to WAF instances across all organizational accounts.
5. Ensure all sub-accounts are members of an organization in the AWS Organizations. Use CloudFormation to implement request restrictions for SQL code on the CloudFront distributions across all accounts. Setup a CloudWatch event to notify administrators if requests with SQL code are seen.

Answer: d

EXPLANATION:

Firewall Manager is a very effective way of managing WAF rules across many WAF instances and accounts. It does require that the accounts be linked as an AWS Organization.

A client calls you in a panic. They notice on their RDS console that one of their mission-critical production databases has an "Available" listed under the Maintenance column. They are extremely concerned that any sort of updates to the database will negatively impact their DB-intensive mission-critical application. They at least want to review the update before it gets applied, but they are not sure when they will get around to that. What do you suggest they do?

1. Apply the maintenance items immediately. AWS validates each update with each customer's RDS instances using a shadow image so there is little risk here.
2. Defer the updates indefinitely until they are comfortable.
3. The maintenance will be automatically performed during the next maintenance window. They have no choice in the matter.
4. Disable the Maintenance Window so the updates will not be applied.
5. Backup the database immediate because the updates could come at any time. If possible, create a Read Replica to act as a standby in case problems are introduced with the update.

Answer: b

EXPLANATION:

For RDS, certain OS updates are marked as Required. If you defer a required update, you receive a notice from Amazon RDS indicating when the update will be performed. Other updates are marked as Available, and these you can defer indefinitely. You can also apply the maintenance items immediately or schedule the maintenance for your next maintenance window.

You are helping an IT organization meet some security audit requirements imposed on them by a prospective customer. The customer wants to ensure their vendors uphold the same security practices as they do before they can become authorized vendors. The organization's assets consist of around 50 EC2 instances all within a single private VPC. The VPC is only accessible via an OpenVPN connection to an OpenVPN server hosted on an EC2 instance in the VPC. The customer's audit requirements disallow any direct exposure to the public internet. Additionally, prospective vendors must demonstrate that they have a proactive method in place to ensure OS-level lvulternatiblity are remediated as soon as possible. Which of the following AWS services will fulfill this requirement?

1. Enable AWS Artifact to periodically scan my instances and prepare a report for the auditors.
2. Enable AWS Shield to protect my instances from unauthorized access.
3. Enable AWS GuardDuty to monitor and remediate threats to my instances.
4. Employ AWS Macie to periodically assess my instances for vulnerabilities and proactively correct gaps.
5. Employ Amazon Inspector to periodically assess applications for vulnerabilities or deviations from best practices.

Answer: e

EXPLANATION:

AWS Macie is a service that attempts to detect confidential data rather than OS vulnerabilities. Since there is no public internet access for the VPC, services like GuardDuty and Shield have limited usefulness. They help protect against external threats versus any OS-level needs. AWS Artifact is simply a document repository and has no monitoring functions. Only AWS Inspector will proactively monitor instances using a database of known vulnerabilities and suggest patches.

You are in the process of migrating a large quantity of small log files to S3 for long-term storage. To accelerate the process and just because you can, you have created quite sophisticated multi-threaded distributed process deployed across 100 VMs which can load hundreds of thousands of files at one time. For some reason, the process seems to be throttled somewhere along the chain. You try many things to try to uncover the source of the throttling but nothing works. Reluctantly, you decide to turn off the KMS encryption setting for your S3 bucket and the throttling goes away. You turn AMS-KMS back on and the throttling is back. Given the troubleshooting steps, what is the most likely cause of the throttling and how can you correct it?

1. You are maxing out your network connection. You must split the traffic over multiple interfaces.
2. You are maxing out your SYNC requests to S3. You need to request a limit increase via a Support Case.
3. You are maxing out your PUT requests to S3. You need to change over to multi-part upload as a workaround.
4. You have exceeded the number of API calls for your account. You must create a new account.
5. You are hitting the KMS encrypt request account limit. You must request a limit increase via a Support Case.

Answer: e

EXPLANATION:

Through a process of elimination, it seems you have identified the variable that is causing the throttling. KMS, like other AWS services, does have rate limiters which can be increased via Support Case.

A client has asked you to review their system architecture in advance of a compliance audit. Their production environment is setup in a single AWS account that can only be accessed through a monitored and audited bastion host. Their EC2 Linux instances currently use AWS-encrypted EBS volumes and the web server instances sit in a private subnet behind an ALB that terminates TLS using a certificate from ACM. All their web servers share a single Security Group, and their application and data layer servers similarly share one Security Group each. Their S3 objects are stored with SSE-S3. The auditors will require all data to be encrypted at rest and will expect the system to secure against the possibility that TLS certificates might be stolen by would-be spoofers. How would you help this client pass their audit in a cost effective way?

1. Continue to use the ACM for the TLS certificate.
2. Leave the S3 objects alone.
3. Deploy CloudHSM and migrate the TLS keys to that service.
4. Encrypt the S3 objects with OpenPGP locally before re-uploading them to S3.
5. Make no changes to the EBS volumes.
6. Reconfigure the EC2 EBS volumes to use LUKS OS-Level encryption.

Answer: a, b, e

EXPLANATION:

All the measures they have taken with Certificate Manager, S3 encryption and the EBS volumes meet the audit requirements. There is no need for LUKS, CloudHSM or client-side encryption.

A client is trying to setup a new VPC from scratch. They are not able to reach the Amazon Linux web server instance launched in their VPC from their on-prem network using a web browser. You have verified the internet gateway is attached and the main route table is configured to route 0.0.0.0/0 to the internet gateway properly. The instance also is being assigned a public IP address. Which of the following would be another potential cause of the problem?

1. The IAM role assigned to the LAMP instances does not have any policies assigned.
2. The instance does not have an elastic IP address assigned.
3. The subnet of the instance is not associated with the main route table.
4. The inbound security group allows port 80 and 22 only.
5. The default route to the internet gateway is incorrect.
6. The customer has disabled the ec2-user account on the Amazon Linux instance.
7. The outbound network ACL allows port 80 and 22 only.

Answer: c, g

EXPLANATION:

For an HTTP connection to be successful, you need to allow port 80 inbound and allow the ephemeral ports outbound. Additionally, it is possible that the subnet is not associate with the route table containing the default route to the internet.

A development team is comprised of 20 different developers working remotely around the globe all in different timezones. They are currently practicing Continuous Delivery and desperately want to mature to true Continuous Deployment. Given a very large codebase and distributed nature of the team, enforcing consistent coding standards has become the top priority. Which of the following would be the most effective to address this problem and get them closer to Continuous Deployment?

1. After integrating and load testing, run a code compliance check against the binary created during the build.
2. Incorporate a code style check right before user interface testing to ensure standards are being followed.
3. Include code style check in the build stage of the deployment pipeline using a linting tool.
4. Introduce a peer review step into their deployment pipeline during the daily stand-up, requiring sign off for each commit.
5. Require all developers to use the Pair Programming feature of Cloud9. The commits must be signed by both developers before merging.
6. Issue a department directive that standards must be followed and require the developers to sign the document.

Answer: c

EXPLANATION:

Including an automated style check prior to the build can move them closer to a fully automated Continuous Deployment process. A style check only before UI testing is too far in the SDLC.

You manage a relatively complex landscape across multiple AZs. You notice that the incoming requests vary mostly depending on the time of day but also there is a more unpredictable component resulting in smaller spikes and valleys for your resources. Fortunately, you manage this landscape via OpsWorks Stacks. What options, if any, are available to you as part of the OpsWorks featureset.

1. If you need the ability to dynamically scale, you will need to use OpsWorks for Chef Automate. OpsWorks Stacks does not support scaling.
2. You would define a baseline level of resources and configure them for 24/7 instances. Then you could define a time-based instances to cover certain times of day. Finally, you could cover the volatile spikes with a load-based instances. All this can be done within OpsWorks Stacks.
3. You can enabled CloudFormation Anticipated Scaling that uses past CloudWatch metrics and machine learning to automatically design a scaling policy optimized for the incoming request patterns.
4. You would define a baseline level of resources within the OpsWorks Stack Console to cover the average load. But for the periodic load, that requires a scheduled auto-scaling policy. Similarly, for the volatile spikes, you must use a stepped auto-scaling policy defined in an auto scaling group.

Answer: b

EXPLANATION:

OpsWorks Stacks offers three types of scaling: 24/7 for instances that remain on all the time; time-based for instances that can be scheduled for a certain time of day and on certain days of the week; and load-based scaling which will add instances based on metrics. All this can be configured from within the OpsWorks Stack console.

You manage a group of EC2 instances that host a critical business application. You are concerned about the stability of the underlying hardware and want to reduce the risk of a single hardware failure impacting multiple nodes. Regarding Placement Groups, which of the following would be the best course of action in this case?

1. You would use the AWS CLI to move the existing instances into a spread placement group.
2. You would the AWS Console to move the existing instances into a clustered placement group.
3. You cannot move existing instances into a new placement group. You would create AMIs from the existing instances and redeploy them into a clustered placement group.
4. You would use the AWS CLI to move the existing instances into a diversified placement group.
5. You would move the instances onto a Dedicated Host.

Answer: a

EXPLANATION:

Spread Placement Groups ensure your instances are each placed on separate underlying hardware so this reduces the risk of a single hardware failure taking down multiple instances.

You have a standard SQS queue to receive messages from the frontend application. The backend application is JAVA based and the AWS SDK is used to get the messages from the queue for processing. The SQS queue is not busy most of the time. According to the backend application logs, there is a high number of empty ReceiveMessageResponse instances returned. You want to adjust the settings to minimize the number of empty responses and reduce the cost. How would you implement this?

1. Consume the messages in the SQS queue using long polling. Set the queue attribute ReceiveMessageWaitTimeSeconds to be more than 0. Amazon SQS will wait until there is an available message in a queue before sending a response.
2. Increase the default visibility timeout of the queue to reduce the possibilities that the messages become visible to consumers again. The application can also use the ChangeMessageVisibility API to specify a suitable timeout value.
3. Modify AWS SDK to get the messages in the SQS queue by short polling. The ReceiveMessage call from the consumer sets the WaitTimeSeconds attribute to 0. As a result, the empty responses are eliminated.
4. Add a delivery delay in the SQS queue such as 1 minute. The delay helps to postpone the delivery of new messages to the queue for some time. When the JAVA application polls the messages from the queue, there will be a lower chance to get an empty response.

Answer: a

EXPLANATION:

Amazon SQS long polling is preferable to short polling in most of the cases. Long polling requests let the consumers receive messages as soon as they arrive in the queue. It can help to reduce the number of empty responses. In order to enable long polling, the attribute ReceiveMessageWaitTimeSeconds should be more than 0. Short polling is incorrect. Visibility timeout and delivery delay do not address the problem of empty responses.

You are a database administrator for a company in the process of changing over from RDS MySQL to Amazon Aurora for MySQL. You setup the new Aurora database in a similar fashion to how your pre-existing RDS MySQL landscape was setup: Multi-AZ with Read Replica in a backup region. You have just completed the migration of data and verified that the new Aurora landscape is performing like it should. You are now in the process of decommissioning the old RDS MySQL landscape. First, you decide to disable automatic backups. Via the console, you try to set the Retention Period to 0 but receive an error saying "Cannot Set Backup Retention Period to 0". How can you disable automatic backups?

1. You cannot disable automatic backups on RDS instances. This feature is built into the platform as a failsafe.
2. You must first reprovision the database as a single AZ instances. Multi-AZ replication requires backups to be enabled.
3. Automatic backups are enabled and disabled at the database engine level. You need to login using a MySQL client to turn off automatic backups.
4. You cannot disable backups via the console. You must do this via the AWS CLI or SDK.
5. Remove the Read Replicas first.

Answer: e

EXPLANATION:

For RDS, Read Replicas require backups for managing read replica logs and thus you cannot set the retention period to 0. You must first remove the read replicas and then you can disable backups.

Your client is a small engineering firm which has decided to migrate their engineering CAD files to the cloud. They currently have an on-prem SAN with 30TB of CAD files and growing at about 1TB a month as they take on new projects. Their engineering workstations are Windows-based and mount the SAN via SMB shares. Propose a design solution that will make the best use of AWS services, be easy to manage and reduce costs where possible.

1. Setup Storage Gateway-File Gateway and configure the CAD workstations to mount as iSCSI. Use a Snowball appliance to sync data daily to S3 buckets at AWS.
2. Order a Snowball appliance to migrate the bulk of the data. Setup an EFS share on AWS and configure the CAD workstations to mount via SMB.
3. Use AWS CLI to sync the CAD files to S3. Setup Storage Gateway-File Gateway locally and configure the CAD workstations to mount as SMB.
4. Use AWS CLI to sync the CAD files to S3. Use EC2 and EBS to create an SMB file server. Configure the CAD workstations to mount the EC2 instances. Setup Direct Connect to ensure performance is acceptable.
5. Order a Snowmobile to migrate the bulk of the data. Setup S3 buckets on AWS to store the data. Use AWS WorkDocs to mount the S3 buckets from the engineering workstations.

Answer: c

EXPLANATION:

At present, EFS doesn't support Windows-based clients. Storage Gateway-File Gateway does support SMB mount points. The other options introduce additional unneeded costs.

You have run out of root disk space on your Windows EC2 instance. What is the most efficient way to solve this?

1. Use AWS System Manager Run service to remotely execute a PowerShell script using AWS Tools for PowerShell to expand the volume using the ModifyInstance command.
2. Compress all files on the root volume using the built-in zip utility. Modern versions of Windows will automatically unzip the files when they are accessed.
3. From the AWS Console, select Modify Volume for the EBS volume. Enter the new size and confirm the change. Connect to your Windows instance and use Disk Manager to extend the newly resized volume.
4. From the AWS CLI, use the "modify-instance" command for EC2 to resize the volume to a larger size. Using RDP, connect to the Windows instances and use Disk Manager to expand the volume.

Answer: c

EXPLANATION:

We can easily increase the size of an EBS from the console or the CLI (using modify-volume) but then we also need to allow the OS to expand the resized volume so we can use it. For Windows Server, we could use Disk Manager.

Your company has an Inventory Control database running on Amazon Aurora deployed as a single Writer role. Over the years more departments have started querying the database and you have scaled up when necessary. Now the Aurora instance cannot be scaled vertically any longer, but demand is still growing. The traffic is 90% Read based. Choose an option from below which would meet the needs of the company in the future.

1. Create multiple additional Readers within the Aurora cluster and alter the application to make use of Read-Write splitting
2. Convert Aurora to a Multi-AZ Deployment in three or more zones
3. Increase the maximum number of connections into the database by changing the max\_connections parameter
4. Use Query plan management to allow the optimizer to choose the most efficient plan for each job and make transactions quicker

Answer: a

EXPLANATION:

This question is about scaling, and if you have scaled up to the maximum level (db.r4.16xlarge) the next step is to consider scaling out. In this case the application is Read heavy, which lends itself perfectly to adding extra Read replicas and using Read-Write splitting to help future growth. Changing the max\_connections value or using Query plan optimisation may make performance more efficient, but they are not long term solutions. Adding Multi-AZ simply adds High Availability.

You are assisting a company in the migration of their container-based web landscape over to Amazon. They have a total of 21 containers which comprise their DEV, QA and Production environments. All environment are identical in design and size. Each environment consists of 3 web servers, 3 app servers and 1 datastore server. Given the landscape, which of the provided options would be best for them to minimize maintenance?

1. Redeploy the web landscape on a MEAN stack under Elastic Beanstalk, making use of auto-scaling groups to right-size the respective environments.
2. Deploy the web, app and database containers using ECS. Make use of Fargate for the underlying ECS infrastructure.
3. Deploy the web, app and database servers using ECS on EC2. Purchase 1-year reserved instance contracts for the required EC2 instances.
4. Deploy the web and app servers in each environment using ECS. Provision an RDS instance for each environment. Use AWS Systems Manager to provide a common management console.

Answer: c

EXPLANATION:

Deploying containers via ECS is a good option but we would want to use the EC2 hosted path. Fargate is generally used for transient workloads and our datastore would be something we'd want to persist. We might be able to deploy the data store with RDS, but the question does not make it clear if the data store is an RDS-supported database. It could be a NoSQL data store or some other database unsupported by RDS. Similarly, a MEAN stack under Elastic Beanstalk might not be compatible with our landscape either.

Across your industry, there has been a rise in activist hackers launching attacks on companies like yours. You want to be prepared in case some group turns its attention toward you. The most common attack, based on forensic work security researchers have done after other attacks, seems to be the TCP Syn Flood attack. To better protect yourself from that style of attack, what is the least cost measure you can take?

1. Subscribe to a Business or Enterprise Support Plan. Engage AWS DDoS Response Team and arrange for a custom mitigation.
2. Implement AWS WAF and configure filters to block cross-site scripting match conditions.
3. This type of attack is automatically addressed by AWS. You do not need to take additional action.
4. Implement AWS Shield Advanced and configure it to generate CloudWatch alarms when malicious activity is detected.
5. Re-architect your landscape to use an application load balancer in front of any public facing services.

Answer: c

EXPLANATION:

AWS Shield Standard is offered to all AWS customers automatically at no charge and will protect against TCP Syn Flood attacks without you having to do anything - this meets the requirements of protecting TCP Syn Flood attacks at the lowest cost possible, as described in the question. A more robust solution which is better aligned to best practice would involve a load balancer in the data path, however as this would provide more functionality than required at a higher cost, is not the correct option for this question.

You've begun deploying EC2 and VMware Cloud on AWS instances to host various applications which you'd like to make accessible to those who authenticate via an on-premises Active Directory domain. You've configured AWS Managed Microsoft AD in the same region as the EC2 and VMware Cloud on AWS instances with a one-way trust back to the corporate AD domain. You're able to seamlessly join new EC2 Windows instances to the Managed AD domain at launch, but the EC2 Linux and VMware Cloud on AWS instances don't show up in the domain when launched. What additional actions need to take place in order to seamlessly join all the instances to the domain at launch?

1. Add inbound rules for the EC2 Linux and the VMware Cloud on AWS instances to allow traffic on port 389 for LDAP
2. Have EC2 Linux instances configure SSH services to allow password authentication, and configure the VMware Cloud NSX Compute Gateway (CGW) to not perform Network Address Translation on the domain server's IP address
3. Have EC2 Linux instances assume a role with permissions to write to the Managed AD domain, and configure the VMware Cloud NSX Compute Gateway (CGW) to pass Active Directory requests through without VMware Tunneling
4. Create a bootstrap script to install a Kerberos client package and perform a Realm Join command for the EC2 Linux instances, and add a VMware Cloud NSX Compute Gateway (CGW) Firewall Rule for the VMware Cloud on AWS instances

Answer: d

EXPLANATION:

A bootstrap script that installs a Kerberos client package and performs a Realm Join will successfully join an EC2 Linux instance to an Active Directory domain. Active Directory uses Kerberos as it's authentication protocol between a server and a client. VMC Compute Gateway (CGW) Firewall Rules block traffic to all uplinks by default, so 'allow' rules need to be added. This particular issue would not be due to a role or Security Group configuration problem because the EC2 Windows instances are able to join the domain successfully. The instance's SSH service does need to be configured to allow password authentication, but this is not necessary for the domain join operation.

You are implementing a new eCommerce system for your organization. It requires Redhat Linux and uses either multicast or external cache (Redis or Memcached) to share sessions. You need to implement SSL but do not want to manage individual certificates on each EC2 instance. Additionally, you want to be sure all parts of the landscape are setup for high availability. Which of the following architectures best fits the situation at the least cost?

1. Use an Application Load Balancer attached to a spot fleet of RHEL. Use ElastiCache for Redis as a session cache. Use Certificate Manager to assign a certificate to the ALB and terminate SSL there.
2. Use ElastiCache for Memcache as a session cache. Use an Application Load Balancer attached to an auto scaling group of RHEL instances. Use Certificate Manager to assign a certificate to the load balancer and terminate SSL there.
3. Use ElastiCache for Memcached as a session cache. Use a Network Load Balancer attached to an auto scaling group of RHEL instances. Use Certificate Manager to assign a certificate to the load balancer and terminate SSL there.
4. Use ElastiCache for Redis as a session cache. Use an Application Load Balancer attached to an auto scaling group of RHEL instances. Use Certificate Manager to assign a certificate to the ALB and terminate SSL there.
5. Use an Application Load Balancer attached to an auto scaling group of RHEL instances. Enable multicast support in the VPC containing the web servers. Use Certificate Manager to assign a certificate to the ALB and terminate SSL there.

Answer: d

EXPLANATION:

Because multicast is not supported in VPCs, we have to use a cache. Redis supports more high availability configurations than Memcached. Exclusive use of a spot fleet could leave us with no running instances, so we avoid that option.

Given an IP CIDR block of 56.23.0.0/24 assigned to a VPC and the single subnet within that VPC for that whole range, how many usable addresses will you have?

1. 4096
2. 251
3. 254
4. You cannot assign the entire CIDR range of a VPC to a single subnet.
5. Zero. You must use a private IP range as defined in RFC1918 for VPCs.

Answer: b

EXPLANATION:

For VPCs and subnets, you can use IP addresses that are in RFC1918 or not. If you choose addresses not in the RFC1918 ranges, you will not be able to route traffic to the internet directly with those addresses. You would have to use a NAT. For a /24 netmask, you can expect 251 usable addresses because of the 5 reserved addresses.

What backup and restore options are available to you when using RDS for Oracle?

1. Oracle Recovery Manager (RMAN)
2. Oracle Data Pump Export and Import
3. Oracle Export/Import Utilities
4. Replication Backups
5. RDS Snapshot and Point In Time Recovery

Answer: b, c, e

EXPLANATION:

Amazon RDS for Oracle can use the standard backup methods for RDS which is Snapshot and Point In Time Recovery. You can also use Data Pump to export logical data to binary files, which you can later import into the database as well as the standard 'exp' and 'imp' utilities. RMAN is not supported in RDS as a backup mechanism, although you can run certain RMAN commands against the database using the rdsadmin.rdsadmin\_rman\_util package. Replication Backups is not a valid function within RDS for Oracle.

You are volunteering with a local STEM (Science, Technology, Engineering and Math) program for youth. You have decided that you'd like to help them learn about AWS by spinning up their very own WordPress site. Given that the youth have no experience with AWS and the program, you want to choose the easiest way for students to spin up a simple webserver. Which AWS technologies would you choose?

1. CloudFormation
2. Lightsail
3. AWS Marketplace
4. ECS
5. VPC
6. EC2

Answer: b

EXPLANATION:

AWS Lightsail is designed to be a very easy entry-level experience for those just starting out with virtual private servers. A WordPress site can be deployed with literally a single click and does not require AWS Console access or knowledge of EC2 or VPCs.

You have been asked to design a landscape that can facilitate the upload very high resolution photos from mobile devices, gather metadata on objects in the photos and store that metadata for analysis. Which of the following components would you use for this use-case for quickest implementation and best scalability?

1. S3
2. EMR
3. DynamoDB
4. Kinesis
5. Rekognition
6. Polly

Answer: a, c, e

EXPLANATION:

DynamoDB and S3 represent the most reasonable and scalable choices in this list for metadata storage (DynamoDB) and file upload (S3). Kinesis has size limits on the inbound object so it would not be appropriate for use cases that involve potentially large files like photos. Amazon Rekognition is image processing service that can extract metadata on objects in a photograph.

You are a developer for an Aerospace company. As part of an outreach and education program, the company has financed the construction of a free public service that provides weather forecasts for the sun. Anyone can make a call to this REST service and receive up-to-date information on forecasted sun flare or sun spots that might have an electromagnetic impact here on Earth. You are in the final stages of developing this new serverless application based on DynamoDB, Lambda and API Gateway. During performance testing, you notice inconsistent response times for the service. You had expected the API to be relatively consistent since its just retrieving data from DynamoDB and returning it as JSON via the API Gateway. What might account for this variation in response time?

1. There are not enough open inbound ports in your VPC.
2. The CloudFront distribution used by API Gateway is not deployed fully yet.
3. You have enabled caching on the API Gateway.
4. You are using HTTP rather than HTTPS.
5. You are experiencing a cold start.
6. Your DynamoDB RCUs are underprovisioned.
7. The data is being updated on DynamoDB at the exact same time you are trying to read it.

Answer: e, e, f

EXPLANATION:

Inconsistent response times can have a few different causes. The exact nature of the testing is not explained but we can anticipate a few causes. If you have enabled API Gateway caching, the gateway can return a result from its cache without having to go back to a supplying service or database. This can result in various response rates depending on if an item is in the cache or not. (The question did not specify we had slow response...just inconsistant response which could be a response faster than we expected.) When a Lambda function is run for the first time or after an update, AWS must provision the Lambda environment and pull in any external dependencies. This can result in a slower response time at first but faster later. Also, if we do not have sufficient RCU for our DynamoDB table, we could run into throttling of the reads which could appear as inconsistent response times.

You work for an organic produce importer and the company is trying to find ways to better engage with its supply chain. One idea is to create a public ledger that all members of the supply chain could update and query as products changed hands along the journey to the customer. Then, your company could create an app that would allow consumers to view the chain from producer to end retailer and have confidence in the product sourcing. Which AWS service or services could most directly help realize this vision?

1. Amazon DynamoDB and Lambda
2. Amazon CloudTrail and API Gateway
3. Amazon Managed Blockchain
4. Amazon P2PShare and API Gateway
5. Amazon QLDB

Answer: e

EXPLANATION:

Amazon Quantum Ledger Database (QLDB) is a fully-managed ledger database that provides a transparent, immutable and verifiable transaction log. While other products could be used to create such a supply chain logging solution, QLDB is the closest to a ready-made solution.

Your client is a software company starting their initial architecture steps for their new multi-tenant CRM application. They are concerned about responsiveness for companies with employees scattered around the globe. Which of the following ideas should you suggest to help with the overall latency of the application?

1. Install the application in several regions around the globe. As new customers and users are on-boarded, pre-cache their user data in CloudFront for that region. Use AWS Batch to routinely expire the cache to ensure the latest updates are visible.
2. Install key parts of the application in multiple AWS regions chosen to balance latency for geographically diverse users. Use Lambda@Edge to dynamically select the appropriate region based on the users location.
3. Store the data in a DynamoDB Global Table. Use an auto scaling ElastiCache cluster with Memcached as a caching layer. Distribute static elements of the application via CloudFront. Use Route 53 Weighted routing to dynamically route users to the nearest region.
4. Install the application on several regions around the globe. Use RDS cross-region read replication for PostgreSQL to ensure a strongly consistent data store.
5. Architect the system to use as many static objects as possible with high TTL. Use CloudFront to retrieve both static and dynamic objects. POST and PUT new data through CloudFront.

Answer: b, e

EXPLANATION:

CloudFront can cache both static and dynamic content. By setting a high TTL, we allow CloudFront to serve content longer before having to refresh from the origin. Additionally, Lambda@Edge can intercept the request and direct the requester to a region based on the geographic origin of the request.

You are in the process of porting over a Java application to Lambda. You find that one Java application's code exceeds the size limit Lambda allows--even when compressed. What can you do?

1. Consider containerization and deploy using Elastic Beanstalk.
2. Change the Java Runtime Version in the Lambda function to one that supports BIGINT.
3. Evaluate the structure of the program and break it into more modular components.
4. Consider using API Gateway to offload some of the I/O your code requirements.
5. Use AWS CodeBuild to identify unused libraries and remove them from the package.
6. Enable Extended Storage in the Lambda console to permit a larger codebase to be deployed.

Answer: a, c

EXPLANATION:

If your code is too large for Lambda, it might indicate the need to break the code down into more atomic elements to support microservice best practices. If breaking the code down is not possible, you should consider deploying in a different way like ECS or Elastic BeanStalk.

You are helping an IT Operations group transition into AWS. They will be created several instances based off the latest Amazon Linux 2 AMI. They are unsure of the best way to enable secure connections for all members of the group and certainly do not want to share credentials. Which of the following methods would you recommend?

* Allow each administrator to create their own SSH keypair and assign them all to the SSH Key for the instance upon each launch.
* Configure IAM role access for AWS Systems Manager Session Manager.
* Allow administrators to update the SSH key of the instance in the AWS console each time they need access to a system.
* Share the single private SSH key with each administrator in the group.
* Create a bastion host and use it like a jump-box. Paste each administrators private key into the known\_hosts file on the bastion host.

Answer: b

EXPLANATION:

Of the provided options, the only one that upholds AWS best practices for providing secure access to EC2 instances is to use AWS Session Manager.

You are advising a client on some recommendations to increase performance of their web farm. You notice that traffic seems to usually spike on the days after public holidays and unfortunately the responsiveness of the web server as collected by a third-party analytics company reflects a customer experience that is slower than targets. Of these choices, which is the best way to improve performance with minimal cost?

1. Create replicas of the existing web farm in multiple regions. Migrate static assets to S3 and use cross-region replication to synchronize across regions. Create CloudFront distributions in each region. Use Route 53 to direct traffic to the closest CloudFront alias based on a geolocation routing policy.
2. Use CloudTrail and SNS to trigger a Lambda function to scale the web farm when network traffic spikes over a configured threshold. Create an additional Internet Gateway and split the traffic equally between the two gateways using an additional route table.
3. Configure a dynamic scaling policy based on network traffic or CPU utilization. Migrate static assets from EBS volumes to S3. Configure two Cloudfront distributions--one for static content and one for dynamic content. Use Route 53 to consolidate both Cloudfront distributions under one alias.
4. Configure a scheduled scaling policy to increase server capacity on days after public holidays.

Answer: d

EXPLANATION:

Of these options, only one meets the question requirements of performance at minimal cost. Simply scheduling a scale event during a known period of traffic is a perfectly valid way to address the requirement and does not incur unnecessary cost. CloudTrail records API access and is not suitable for network alarms. Route 53 would not be able to "consolidate" dynamic and static web resources.

You work for a specialty retail organization. They are building out their AWS VPC for running a few applications. They store sensitive customer information in two different encrypted S3 buckets. The applications running in the VPC access, store and process sensitive customer information by reading from and writing to both the S3 buckets. The company is also using a hybrid approach and has several workloads running on-premises. The on-premises datacenter is connected to their AWS VPC using Direct Connect. You have proposed that an S3 VPC Endpoint be created to access the two S3 buckets from the VPC so that sensitive customer data is not exposed to the internet. Select two correct statements from the following that relate to designing this solution using VPC Endpoint.

1. Bucket policies on the two S3 buckets can specify the id of each VPC Endpoint using AWS attribute sourceVpce to further restrict which S3 buckets can be accessed by the VPC Endpoint
2. Bucket policies on the two S3 buckets can specify the id of each VPC Endpoint using AWS attribute sourceVpce to further restrict which VPC Endpoints can access each bucket
3. You need two VPC Endpoints, one for each S3 bucket, as a single VPC Endpoint can only access a single S3 bucket
4. Each VPC Endpoint is a Gateway Endpoint that also requires correct routes in the Route Table associated with each subnet that wants to access the endpoint

Answer: b, d

EXPLANATION:

S3 VPC Endpoint is a common topic tested in the SA-P Exam, as it enables S3 access over a private network, which is a common security requirement in many organizations. It is also a cost-effective way to establish outbound connection to S3, as the alternative is to use NAT Gateways, which are charged by the hour even if there is no traffic using them. On vertical scanning of the answer choices, it should be obvious that one of the two closely worded choices is correct, and one of the other two choices is correct as well. That is because if there are 2 or 3 or 4 closely worded choices, only one (or in some rare cases, two) is correct - this is a common pattern in the SA-P test. For the closely worded pair - the bucket policy of an S3 bucket will always specify who can or cannot access the bucket. It will not dictate how a VPC Endpoint behaves. Hence, the choice that suggests that a bucket policy can control a VPC Endpoint is incorrect. Between the other two choices, remember that a VPC Endpoint can connect to any number of S3 buckets by default. One Endpoint for each bucket is simply not scalable, and should stand out as incorrect. The remaining choice is correct because the S3 VPC Endpoint is of type Gateway Endpoint as opposed to Interface Endpoint, and a subnet needs Routes in the Routing Table for sources in the subnet to be able to connect to it. Read the links provided to understand the differences

To be sure costs of AWS resources are allocated to the proper budgets, you are trying to come up with a way to allocate the AWS bill to the proper cost centers. Which of the following would be most effective for your organization?

1. Make use of AWS Artifact to analyse the spending pattern over the month and identify the IAM users responsible for the most costs. Cross-reference that with the cost centers to which IAM users belong.
2. Use an SCP at the organizational level to require a cost center tag be applied to every resource. Activate the cost center tag in the Billing Console and allocate costs based on that.
3. Use API Gateway to create a proxy for the API of the resources your users will deploy. Insert some custom logic using VTL to automatically append a cost center tag to the request based on the cost center of the IAM user making the request.
4. Use AWS Batch to periodically run a custom Lambda function that scans all resources and deletes any without proper tagging for cost center.
5. Deploy products within AWS Service Catalog and only allow users to deploy resources using the catalog. Use TagOptions to provide the users a list from which they can select their cost center. Activate the cost center tag in the Billing Console.

Answer: e

EXPLANATION:

Using Service Catalog is a good way to automatically enforce and apply a tagging strategy and it requires no special effort from the product consumers.

Which of the following is an example of buffer-based approach to controlling costs?

1. A mobile image upload and processing service makes use of SQS to smooth an erratic demand curve.
2. An auto-scaling fleet is created to dynamically adjust available compute resources based network connection events as reported by CloudWatch.
3. A public-facing API is created using API Gateway and Lambda. As a serverless architecture, it scales seamlessly in step with demand.
4. A production ERP landscape is scaled up during the month-end financial close period to provide some padding for the additional processing and reports so they do not impact the normal business processes.

Answer: a

EXPLANATION:

The buffer-based approach to controlling costs is discussed in the Cost Optimization Pillar of the AWS Well-Architected Framework. A buffer is a mechanism to ensure that applications can communicate with each other when they are running at different rates over time. By decoupling the throughput rate of a process, you can better govern and smooth demand--creating a less volatile and reactionary landscape. As a result, costs can be reduced by optimizing for the steady state.

Your company has been running its core application on a fleet of r4.xlarge EC2 instances for a year. You are confident that the application has a steady-state performance and now you have been asked to purchase Reserved Instances (RIs) for a further 2 years to cover the existing EC2 instances, with the option of moving to other Memory or Compute optimised instance families when they are introduced. You also need to have the option of moving Regions in the future. Which of the following options meet the above criteria whilst offering the greatest flexibility and maintaining the best value for money.

1. Purchase a 1 year Standard Zonal RI for 3 years, then sell the unused RI on the Reserved Instance Marketplace
2. Purchase a 1 year Convertible RI for each EC2 instance, for 2 consecutive years running
3. Purchase a Scheduled RI for 3 years, then sell the unused RI on the Reserved Instance Marketplace
4. Purchase a Convertible RI for 3 years, then sell the unused RI on the Reserved Instance Marketplace

Answer: b

EXPLANATION:

When answering this question, it's important to exclude those options which are not relevant, first. The question states that the RI should allow for moving between instance families and this immediately rules out Standard and Scheduled RIs as only Convertible RIs can do this. Of the 2 Convertible RI options, one can be ruled out as it suggests selling unused RI capacity on the Reserved Instance Marketplace, but this is not available for Convertible RIs and therefore that only leaves one answer as being correct.

Which of the following activities will have the most cost impact (increase or decrease) on your AWS bill?

1. Add a new Route 53 hosted zone.
2. Provision an Elastic IP and associate it to a running instance.
3. Deploy existing reserved instances into a Placement Group.
4. Begin using AWS OpsWorks Stacks on EC2 to manage your landscape
5. Start using AWS App Mesh to improve the stability of your existing service landscape.

Answer: a

EXPLANATION:

Provisioning an EIP to a running instance or using Placement Groups or App Mesh all do not cost anything. OpsWorks Stacks on EC2 does not cost anything but using it for on-prem systems does cost a small amount. The only thing on this list that would increase your AWS bill is adding a Route 53 hosted zone.

You are helping a Retail client migrate some of their assets over to AWS. Presently, they are in the process of moving their Enterprise Data Warehouse. They are planning to re-host their very large Oracle data warehouse on EC2 in a high availability configuration across AZs. They presently have several Scala scripts that process some detailed Point of Sale data that is collected each day. The scripts perform some aggregation on the data and import the aggregate into their Oracle database. They want to move this process to AWS as well. Which option would be the most cost-effective way for them to do this?

1. Migrate the processing to AWS EMR.
2. Import your Scala scripts into AWS SCT for processing.
3. Migrate from Oracle to Redshift and use Kinesis Firehose.
4. Create Lambda functions using your Scala scripts.
5. Migrate the processing to AWS Glue.

Answer: e

EXPLANATION:

AWS Glue is a fully managed extract, translate and loading service and is compatible with Scala. EMR could do this but represents more overhead than necessary. Lambda is not compatible with Scala and migrating to Redshift does not bring anything in this case if the customer wants to retain their Oracle database.

Due to a dispute with their co-location hosting company, your client is forced to move some applications as soon as possible to AWS. The main application uses IBM DB2 for the data store layer and a Java process on AIX which interacts via JMS with IBM MQ hosted on an AS400. What is the best course of action to reduce risk and allow for fast migration?

1. Install DB2 on an EC2 instance and migrate the data by doing an export and import. Spin up an instance of Amazon MQ in place of IBM MQ. Install the Java process on a Linux-based EC2 system.
2. Use a physical-to-virtual tool to convert the AIX DB2 server into a virtual machine. Use AWS CLI to import the VM into AWS and launch the VM. Deploy the Java program as a Lambda function. Launch a version of IBM MQ from the AWS Marketplace.
3. Deploy the Java processes as Lambda functions. Install DB2 on an EC2 instance and migrate the data by doing an export and import.
4. Install DB2 on an EC2 instance and use DMS to migrate the data. Encapsulate the Java program in a Docker container and deploy it on ECS. Spin up an instance of Amazon MQ.
5. Use DMS and SCT to migrate DB2 to Aurora. Update the Java application to use SQS and install it on a LInux-based EC2 system.

Answer: a

EXPLANATION:

For a fast migration with minimal risk, we would be looking for a lift-and-shift approach and not spend any time on re-architecting or re-platforming that we don't absolutely have to do. Amazon MQ is JMS compatible and would provide a shorter path to the cloud than SQS. DMS does not support DB2 as a target.

You are consulting with a company who is at the very early stages of their cloud journey. As a framework to help work through the process, you introduce them to the Cloud Adoption Framework. They read over the CAF and come back with a list of activities as next steps. They are asking you to validate these activities to keep them focused. Of these activities, which would you recommend delaying until later in the project?

1. Work with the Human Resources business partners to create new job roles, titles and compensation/remuneration scales.
2. Work with Marketing business partners to design an external communications strategy to be used during potential outages during the migration.
3. Work with internal Finance business partners to design a transparent chargeback model.
4. Hold a workshop with IT business partners about the creation of an IT Service Catalog concept.
5. Investigate the need for training for Program and Project Management staff around agile project management.

Answer: b

EXPLANATION:

External communication usually comes much later in the process once project plans are defined and specific customer impact is better understood.

An automotive supply company has decided to migrate their online ordering application to AWS. The application leverages a Model-View-Controller architecture with the user interface handled by a Tomcat server and twenty thousand lines of Java Servlet code. Business logic also resides in two thousand lines of PL/SQL stored procedure code in an Oracle database. The company's technology leadership has directed your team to move the database to a more cost-effective offering, and to adopt a more cloud-native architecture. Business objectives dictate that the application must be live in the AWS cloud in sixty days. Which migration approach will provide the most scalable architecture and meet the schedule objectives?

1. Migrate the Tomcat server and Servlet code to EC2. Use AWS Database Migration Service to move the application data into Amazon Aurora. Convert the stored procedure code to AWS Lambda Python functions, and modify the Servlet code to invoke them
2. Convert the Servlet Code to JavaScript Lambda functions accessed through Amazon API Gateway. Use AWS Database Migration Service and the AWS Schema Conversion Tool to migrate the application data and stored procedures to Amazon Aurora
3. Migrate the Tomcat server and Servlet code to EC2. Use AWS Database Migration Service and the AWS Schema Conversion Tool to migrate the application data and stored procedures to Amazon Aurora
4. Convert the Servlet Code to JavaScript Lambda functions accessed through Amazon API Gateway. Use AWS Database Migration Service to migrate the application data and stored procedures to an Amazon RDS Oracle instance

Answer: a

EXPLANATION:

This solution will require trade-offs between schedule requirements and architectural desires. Converting twenty thousand lines of Model-View-Controller code to a serverless architecture in sixty days is unreasonable, so moving the Tomcat MVC as-is to EC2 for the initial migration is the best approach. We can migrate to a serverless user interface in a later phase. Database Migration Service will suit our needs well for moving the application data to Aurora, but the most scalable architecture strategy is to migrate the stored procedure code out of the database so that database nodes won't need to be resized when the business logic needs more compute resources. Under normal circumstances, recoding two thousand lines of PL/SQL code to Python Lambda functions within a sixty day time frame will not be a problem.

You have been asked to give employees the simplest way of accessing the corporate intranet and other internal resources, from their iPhone or iPad. The solution should allow access via a Web browser, authentication via SAML integration and you need to ensure that no corporate data is cached on their device. Which option would meet all of these requirements?

1. Tunnel through a Bastion Host into your VPC and view all internal servers via a Web Browser
2. Configure Amazon WorkLink and connect to the servers using a Web Browser with the link provided
3. Connect into the VPC where the internal servers are located using Amazon Client VPN and view the sites using a Web Browser
4. Place all internal servers in a public subnet and lock down access via Security Groups to the IP address of each mobile user

Answer: b

EXPLANATION:

Amazon WorkLink is a fully managed, cloud-based service that enables secure access to internal websites and apps from mobile devices. It provides single URL access to the applications and also links to existing SAML-based identity providers. Amazon WorkLink does not store or cache data on user devices as the web content is rendered in AWS and sent to user devices as encrypted Scalable Vector Graphics (SVG). WorkLink meets all of the requirements in the question and is therefore the only correct answer.

AWS Cost Management encompasses a number of services to help you to organize, control and optimize your AWS costs and usage. Which of the following Cost Management related tools gives you the ability to set alerts when costs or usage are exceeded?

1. AWS Cost & Usage Report
2. AWS Budgets
3. Reserved Instance Reporting
4. AWS Cost Explorer

Answer: b

EXPLANATION:

The correct answer is AWS Budgets. AWS Cost Explorer lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost & Usage Report lists AWS usage for each service category used by an account and its IAM users and finally, Reserved Instance Reporting provides a number of RI-specific cost management solutions to help you better understand and manage RI Utilization and Coverage.

A financial services company operates in all fifty U.S. states. They've decided to deploy part of their application portfolio in the AWS us-east-1, us-east-2, and us-west-2 regions. Multiple AWS accounts will be created, one for each of the company's four business units. The applications need to be able to communicate with each other across the accounts and across the regions. The applications also need to communicate with systems in the corporate data center. Which networking approach with provide the best operational efficiency?

1. Route the AWS cross-account, cross-region traffic through the corporate data center network via VPN connections to leverage existing network infrastructure
2. Create VPC Peering connections between the VPCs in the different regions and different accounts. Use AWS Direct Connect Gateway to interface the corporate data center network to the different AWS regions
3. Deploy an AWS Transit Gateway as a network hub to manage the connections between the VPCs in the different regions, the different accounts, and the corporate data center network
4. Deploy a transit VPC in a shared account with EC2-based appliances that create hub-and-spoke VPN connections to VPCs in the other accounts, the other regions, and the corporate data center network

Answer: c

EXPLANATION:

Creating a hub-and-spoke network topology minimizes network management overhead. Transit Gateway would be the best approach. Routing AWS traffic for many VPCs through Transit Gateway is now possible and will allow for smooth integration of environments without the technical overhead of managing separate VPN or multiple Direct Connect connections.

You are helping a client consolidate several separate accounts into a single account. This consolidation will result in approximately 50 new VPCs in their one account. They want to continue to use Route 53 for DNS but only want it accessable privately. How can you accomplish this most efficiently?

1. Create a Public Hosted Zone within Route 53 and associate it to each VPC. Configure a NACL on each VPC to deny inbound DNS queries (UDP port 53).
2. Create a Private Hosted Zone within Route 53. As the new VPCs are created, associate them with the Private Hosted Zone.
3. Create a central DNS server using EC2 and BIND. Configure Route 53 to reference this DNS server as a resolver. Update DNS records at the registrar to point to the central DNS.
4. Create a Private Hosted Zone within Route 53 for each respective VPC. Configure replication between the private hosted zones to keep records in sync.
5. Install BIND on an EC2 instance in a single VPC. Create VPC peering connections between the DNS VPC and any new VPCs. Configure a DHCP Option Set to assign a DNS and link that to each VPC.

Answer: b

EXPLANATION:

Private Hosted Zones provide DNS services to VPCs but cannot be access from the internet. They can be associated with VPCs either by the console, CLI or programmatically via SDK.