# Amazon.Premium.AWS DevOps Engineer Professional.by.VCEplus.528q

Number: AWS VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 14.7


**Exam Code: AWS DevOps Engineer Professional**
**Exam Name: AWS DevOps Engineer Professional**
**Certification Provider: Amazon**
**Corresponding Certification: AWS DevOps Engineer Professional**
**Website:** https://vceplus.com - https://vceplus.co
**Free Exam:** https://vceplus.com/exam-aws-devops-engineer-professional/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in AWS DevOps Engineer Professional exam products and you get latest questions. We strive to deliver the best AWS DevOps Engineer Professional exam product for top grades in your first attempt.

**Website:** https://vceplus.com - https://vceplus.co
**VCE to PDF Converter:** https://vceplus.com/vce-to-pdf/
**Facebook:** https://www.facebook.com/VCE.For.All.VN/
**Twitter :** https://twitter.com/VCE_Plus

**Exam A**

**QUESTION 1**
To run an application, a DevOps Engineer launches an Amazon EC2 instances with public IP addresses in a public subnet. A user data script obtains the application artifacts and installs them on the instances upon launch. A change to the security classification of the application now requires the instances to run with no access to the Internet. While the instances launch successfully and show as healthy, the application does not seem to be installed. Which of the following should successfully install the application while complying with the new rule?

A. Launch the instances in a public subnet with Elastic IP addresses attached. Once the application is installed and running, run a script to disassociate the Elastic IP addresses afterwards.
B. Set up a NAT gateway. Deploy the EC2 instances to a private subnet. Update the private subnet's route table to use the NAT gateway as the default route.
C. Publish the application artifacts to an Amazon S3 bucket and create a VPC endpoint for S3. Assign an IAM instance profile to the EC2 instances so they can read the application artifacts from the S3 bucket.
D. Create a security group for the application instances and whitelist only outbound traffic to the artifact repository. Remove the security group rule once the install is complete.

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

**Explanation/Reference:**



**QUESTION 2**
An IT department manages a portfolio with Windows and Linux (Amazon and Red Hat Enterprise Linux) servers both on-premises and on AWS. An audit reveals that there is no process for updating OS and core application patches, and that the servers have inconsistent patch levels.
Which of the following provides the MOST reliable and consistent mechanism for updating and maintaining all servers at the recent OS and core application patch levels?

A. Install AWS Systems Manager agent on all on-premises and AWS servers. Create Systems Manager Resource Groups. Use Systems Manager Patch Manager with a preconfigured patch baseline to run scheduled patch updates duringmaintenance windows.
B. Install the AWS OpsWorks agent on all on-premises and AWS servers. Create an OpsWorks stack with separate layers for each operating system, and get a recipe from the Chef supermarket to run the patch commands for each layerduring maintenance windows.
C. Use a shell script to install the latest OS patches on the Linux servers using yum and schedule it to run automatically using cron. Use Windows Update to automatically patch Windows servers.
D. Use AWS Systems Manager Parameter Store to securely store credentials for each Linux and Windows server. Create Systems Manager Resource Groups. Use the Systems Manager Run Command to remotely deploy patch updatesusing the credentials in Systems Manager Parameter Store

**Correct Answer:** D

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

**Explanation/Reference:**

**QUESTION 3**
A company is setting up a centralized logging solution on AWS and has several requirements. The company wants its Amazon CloudWatch Logs and VPC Flow logs to come from different sub accounts and to be delivered to a single auditing account. However, the number of sub accounts keeps changing. The company also needs to index the logs in the auditing account to gather actionable insight. How should a DevOps Engineer implement the solution to meet all of the company's requirements?

A. Use AWS Lambda to write logs to Amazon ES in the auditing account. Create an Amazon CloudWatch subscription filter and use Amazon Kinesis Data Streams in the sub accounts to stream the logs to the Lambda function deployed inthe auditing account.
B. Use Amazon Kinesis Streams to write logs to Amazon ES in the auditing account. Create a CloudWatch subscription filter and use Kinesis Data Streams in the sub accounts to stream the logs to the Kinesis stream in the auditingaccount.
C. Use Amazon Kinesis Firehose with Kinesis Data Streams to write logs to Amazon ES in the auditing account. Create a CloudWatch subscription filter and stream logs from sub accounts to the Kinesis stream in the auditing account.
D. Use AWS Lambda to write logs to Amazon ES in the auditing account. Create a CloudWatch subscription filter and use Lambda in the sub accounts to stream the logs to the Lambda function deployed in the auditing account.



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

**Explanation/Reference:**

**QUESTION 4**
A company wants to use a grid system for a proprietary enterprise in-memory data store on top of AWS. This system can run in multiple server nodes in any Linux-based distribution. The system must be able to reconfigure the entire cluster every time a node is added or removed. When adding or removing nodes, an /etc./cluster/nodes.config file must be updated, listing the IP addresses of the current node members of that cluster The company wants to automate the task of adding new nodes to a cluster. What can a DevOps Engineer do to meet these requirements?

A. Use AWS OpsWorks Stacks to layer the server nodes of that cluster. Create a Chef recipe that populates the content of the /etc/cluster/nodes.config file and restarts the service by using the current members of the layer. Assign thatrecipe to the Configure lifecycle event.
B. Put the file nodes.config in version control. Create an AWS CodeDeploy deployment configuration and deployment group based on an Amazon EC2 tag value for the cluster nodes. When adding a new node to the cluster, update the filewith all tagged instances, and make a commit in version control. Deploy the new file and restart the services.
C. Create an Amazon S3 bucket and upload a version of the etc/cluster/nodes.config file. Create a crontab script that will poll for that S3 file and download it

frequently. Use a process manager, such as Monit or systemd, to restart thecluster services when it detects that the new file was modified. When adding a node to the cluster, edit the file's most recent members. Upload the new file to the S3 bucket.

D. Create a user data script that lists all members of the current security group of the cluster and automatically updates the /etc/cluster/nodes.config file whenever a new instance is added to the cluster

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

**Explanation/Reference:**

**QUESTION 5**
A company has established tagging and configuration standards for its infrastructure resources running on AWS. A DevOps Engineer is developing a design that will provide a near-real-time dashboard of the compliance posture with the ability to highlight violations.
Which approach meets the stated requirements?

A. Define the resource configurations in AWS Service Catalog, and monitor the AWS Service Catalog compliance and violations in Amazon CloudWatch. Then, set up and share a live CloudWatch dashboard. Set up Amazon SNSnotifications for violations and corrections.

B. Use AWS Config to record configuration changes and output the data to an Amazon S3 bucket. Create an Amazon QuickSight analysis of the dataset, and use the information on dashboards and mobile devices.

C. Create a resource group that displays resources with the specified tags and those without tags. Use the AWS Management Console to view compliant and non-compliant resources.

D. Define the compliance and tagging requirements in Amazon inspector. Output the results to Amazon CloudWatch Logs. Build a metric filter to isolate the monitored elements of interest and present the data in a CloudWatch dashboard.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/answers/configuration-management/aws-infrastructure-configuration-management/

**QUESTION 6**
A production account has a requirement that any Amazon EC2 instance that has been logged into manually must be terminated within 24 hours. All applications in the production account are using Auto Scaling groups with Amazon CloudWatch Logs agent configured.
How can this process be automated?

A. Create a CloudWatch Logs subscription to an AWS Step Functions application. Configure the function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned. Then create aCloudWatch Events rule to trigger a second AWS Lambda function once a day that

will terminate all instances with this tag.

B. Create a CloudWatch alarm that will trigger on the login event. Send the notification to an Amazon SNS topic that the Operations team is subscribed to, and have them terminate the EC2 instance within 24 hours.

C. Create a CloudWatch alarm that will trigger on the login event. Configure the alarm to send to an Amazon SQS queue. Use a group of worker instances to process messages from the queue, which then schedules the AmazonCloudWatch Events rule to trigger.

D. Create a CloudWatch Logs subscription in an AWS Lambda function. Configure the function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned. Create a CloudWatch Events ruleto trigger a daily Lambda function that terminates all instances with this tag.

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

**Explanation/Reference:**

**QUESTION 7**
A DevOps Engineer is implementing a mechanism for canary testing an application on AWS. The application was recently modified and went through security, unit, and functional testing. The application needs to be deployed on an AutoScaling group and must use a Classic Load Balancer. Which design meets the requirement for canary testing?



A. Create a different Classic Load Balancer and Auto Scaling group for blue/green environments. Use Amazon Route 53 and create weighted A records on Classic Load Balancer.

B. Create a single Classic Load Balancer and an Auto Scaling group for blue/green environments. Use Amazon Route 53 and create A records for Classic Load Balancer IPs. Adjust traffic using A records.

C. Create a single Classic Load Balancer and an Auto Scaling group for blue/green environments. Create an Amazon CloudFront distribution with the Classic Load Balancer as the origin. Adjust traffic using CloudFront.

D. Create a different Classic Load Balancer and Auto Scaling group for blue/green environments. Create an Amazon API Gateway with a separate stage for the Classic Load Balancer. Adjust traffic by giving weights to this stage.

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

**Explanation/Reference:**

**QUESTION 8**
An online retail company based in the United States plans to expand its operations to Europe and Asia in the next six months. Its product currently runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. All

data is stored in an Amazon Aurora database instance.
When the product is deployed in multiple regions, the company wants a single product catalog across all regions, but for compliance purposes, its customer information and purchases must be kept in each region. How should the company meet these requirements with the LEAST amount of application changes?

A. Use Amazon Redshift for the product catalog and Amazon DynamoDB tables for the customer information and purchases.
B. Use Amazon DynamoDB global tables for the product catalog and regional tables for the customer information and purchases
C. Use Aurora with read replicas for the product catalog and additional local Aurora instances in each region for the customer information and purchases.
D. Use Aurora for the product catalog and Amazon DynamoDB global tables for the customer information and purchases.

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

**Explanation/Reference:**

**QUESTION 9**
A company has several AWS accounts. The accounts are shared and used across multiple teams globally, primarily for Amazon EC2 instances. Each EC2 instance has tags for team, environment, and cost center to ensure accurate cost allocations.
How should a DevOps Engineer help the teams audit their costs and automate infrastructure cost optimization across multiple shared environments and accounts?



A. Set up a scheduled script on the EC2 instances to report utilization and store the instances in an Amazon DynamoDB table. Create a dashboard in Amazon QuickSight with DynamoDB as the source data to find underutilized instances.Set up triggers from Amazon QuickSight in AWS Lambda to reduce underutilized instances.
B. Create a separate Amazon CloudWatch dashboard for EC2 instance tags based on cost center, environment, and team, and publish the instance tags out using unique links for each team. For each team, set up a CloudWatch Eventsrule with the CloudWatch dashboard as the source, and set up a trigger to initiate an AWS Lambda function to reduce underutilized instances.
C. Create an Amazon CloudWatch Events rule with AWS Trusted Advisor as the source for low utilization EC2 instances. Trigger an AWS Lambda function that filters out reported data based on tags for each team, environment, and costcenter, and store the Lambda function in Amazon S3. Set up a second trigger to initiate a Lambda function to reduce underutilized instances.
D. Use AWS Systems Manager to track instance utilization and report underutilized instances to Amazon CloudWatch. Filter data in CloudWatch based on tags for team, environment, and cost center. Set up triggers from CloudWatch into
AWS Lambda to reduce underutilized instances

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

**Explanation/Reference:**
Reference:https://github.com/aws/Trusted-Advisor-Tools/tree/master/LowUtilizationEC2Instances

**QUESTION 10**
A company has a hybrid architecture solution in which some legacy systems remain on-premises, while a specific cluster of servers is moved to AWS. The company cannot reconfigure the legacy systems, so the cluster nodes must have a
fixed hostname and local IP address for each server that is part of the cluster. The DevOps Engineer must automate the configuration for a six-node cluster with high availability across three Availability Zones (AZs), placing two elastic network interfaces in a specific subnet for each AZ. Each node's hostname and local IP address should remain the same between reboots or instance failures.
Which solution involves the LEAST amount of effort to automate this task?

A. Create an AWS Elastic Beanstalk application and a specific environment for each server of the cluster. For each environment, give the hostname, elastic network interface, and AZ as input parameters. Use the local health agent to namethe instance and attach a specific elastic network interface based on the current environment.
B. Create a reusable AWS CloudFormation template to manage an Amazon EC2 Auto Scaling group with a minimum size of 1 and a maximum size of 1. Give the hostname, elastic network interface, and AZ as stack parameters. Use thoseparameters to set up an EC2 instance with EC2 Auto Scaling and a user data script to attach to the specific elastic network interface. Use CloudFormation nested stacks to nest the template six times for a total of six nodes needed for the cluster, and deploy using the master template.
C. Create an Amazon DynamoDB table with the list of hostnames subnets, and elastic network interfaces to be used. Create a single AWS CloudFormation template to manage an Auto Scaling group with a minimum size of 6 and amaximum size of 6. Create a programmatic solution that is installed in each instance that will lock/release the assignment of each hostname and local IP address, depending on the subnet in which a new instance will be launched.
D. Create a reusable AWS CLI script to launch each instance individually, which will name the instance, place it in a specific AZ, and attach a specific elastic network interface. Monitor the instances and in the event of failure, replace themissing instance manually by running the script again.

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

**Explanation/Reference:**

**QUESTION 11**
An education company has a Docker-based application running on multiple Amazon EC2 instances in an Amazon ECS cluster. When deploying a new version of the application, the Developer, pushes a new image to a private Docker container registry, and then stops and starts all tasks to ensure that they all have the latest version of the application. The Developer discovers that the new tasks are occasionally running with an old image. How can this issue be prevented?

A. After pushing the new image, restart ECS Agent, and then start the tasks.
B. Use "latest" for the Docker image tag in the task definition.
C. Update the digest on the task definition when pushing the new image.

D. Use Amazon ECR for a Docker container registry.

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

**Explanation/Reference:**
Explanation:
When a new task starts, the Amazon ECS container agent pulls the latest version of the specified image and tag for the container to use. However, subsequent updates to a repository image are not propagated to already running tasks.

Reference:
https://docs.aws.amazon.com/en_us/AmazonECS/latest/developerguide/task_definition_paramet ers.html

**QUESTION 12**
A financial institution provides security-hardened AMIs of Red Hat Enterprise Linux 7.4 and Windows Server 2016 for its application teams to use in deployments. A DevOps Engineer needs to implement an automated daily check of each AMI to monitor for the latest CVE.
How should the Engineer implement these checks using Amazon Inspector?

A. Install the Amazon Inspector agent in each AMI. Configure AWS Step Functions to launch an Amazon EC2 instance for each operating system from the hardened AMI, and tag the instance with SecurityCheck: True. Once EC2 instanceshave booted up, Step Functions will trigger an Amazon Inspector assessment for all instances with the tag SecurityCheck: True. Implement a scheduled Amazon CloudWatch Events rule that triggers Step Functions once each day.
B. Tag each AMI with SecurityCheck: True. Configure AWS Step Functions to first compose an Amazon Inspector assessment template for all AMIs that have the tag SecurityCheck: True and second to make a call to the Amazon InspectorAPI action StartAssessmentRun. Implement a scheduled Amazon CloudWatch Events rule that triggers Step Functions once each day.
C. Tag each AMI with SecurityCheck: True. Implement a scheduled Amazon Inspector assessment to run once each day for all AMIs with the tag SecurityCheck: True. Amazon Inspector should automatically launch an Amazon EC2instance for each AMI and perform a security assessment.
D. Tag each instance with SecurityCheck: True. Implement a scheduled Amazon Inspector assessment to run once each day for all instances with the tag SecurityCheck: True. Amazon Inspector should automatically perform an in-placesecurity assessment for each AMI.

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

**Explanation/Reference:**

**QUESTION 13**
A Development team uses AWS CodeCommit for source code control. Developers apply their changes to various feature branches and create pull requests to

move those changes to the master branch when they are ready for production. A direct push to the master branch should not be allowed. The team applied the AWS managed policy AWSCodeCommitPowerUser to the Developers' IAM Rote, but now members are able to push to the master branch directly on every repository in the AWS account.
What actions should be taken to restrict this?

A. Create an additional policy to include a deny rule for the codecommit: GitPush action, and include a restriction for the specific repositories in the resource statement with a condition for the master reference.
B. Remove the IAM policy and add an AWSCodeCommitReadOnly policy. Add an allow rule for the codecommit: GitPush action for the specific repositories in the resource statement with a condition for the master reference.
C. Modify the IAM policy and include a deny rule for the codecommit: GitPush action for the specific repositories in the resource statement with a condition for the master reference.
D. Create an additional policy to include an allow rule for the codecommit: GitPush action and include a restriction for the specific repositories in the resource statement with a condition for the feature branches reference.

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

**Explanation/Reference:**
Reference:
https://aws.amazon.com/pt/blogs/devops/refining-access-to-branches-in-aws-codecommit/



**QUESTION 14**
A Developer is designing a continuous deployment workflow for a new Development team to facilitate the process for source code promotion in AWS. Developers would like to store and promote code for deployment from development to production while maintaining the ability to roll back that deployment if it fails. Which design will incur the LEAST amount of downtime?

A. Create one repository in AWS CodeCommit. Create a development branch to hold merged changes. Use AWS CodeBuild to build and test the code stored in the development branch triggered on a new commit. Merge to the master anddeploy to production by using AWS CodeDeploy for a blue/green deployment.
B. Create one repository for each Developer in AWS CodeCommit and another repository to hold the production code. Use AWS CodeBuild to merge development and production repositories, and deploy to production by using AWSCodeDeploy for a blue/green deployment.
C. Create one repository for development code in AWS CodeCommit and another repository to hold the production code. Use AWS CodeBuild to merge development and production repositories, and deploy to production by using AWSCodeDeploy for a blue/green deployment.
D. Create a shared Amazon S3 bucket for the Development team to store their code. Set up an Amazon CloudWatch Events rule to trigger an AWS Lambda function that deploys the code to production by using AWS CodeDeploy for ablue/green deployment.

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

**Explanation/Reference:**

**QUESTION 15**
A DevOps Engineer discovered a sudden spike in a website's page load times and found that a recent deployment occurred. A brief diff of the related commit shows that the URL for an external API call was altered and the connecting port changed from 80 to 443. The external API has been verified and works outside the application. The application logs show that the connection is now timing out, resulting in multiple retries and eventual failure of the call. Which debug steps should the Engineer take to determine the root cause of the issue'?

A. Check the VPC Flow Logs looking for denies originating from Amazon EC2 instances that are part of the web Auto Scaling group. Check the ingress security group rules and routing rules for the VPC.
B. Check the existing egress security group rules and network ACLs for the VPC. Also check the application logs being written to Amazon CloudWatch Logs for debug information.
C. Check the egress security group rules and network ACLs for the VPC. Also check the VPC flow logs looking for accepts originating from the web Auto Scaling group.
D. Check the application logs being written to Amazon CloudWatch Logs for debug information. Check the ingress security group rules and routing rules for the VPC.

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



**Explanation/Reference:**

**QUESTION 16**
An Engineering team manages a Node.js e-commerce application. The current environment consists of the following components:
- Amazon S3 buckets for storing content
- Amazon EC2 for the front-end web servers
- AWS Lambda for executing image processing
- Amazon DynamoDB for storing session-related data
The team expects a significant increase in traffic to the site. The application should handle the additional load without interruption. The team ran initial tests by adding new servers to the EC2 front-end to handle the larger load, but the instances took up to 20 minutes to become fully configured. The team wants to reduce this configuration time.
What changes will the Engineering team need to implement to make the solution the MOST resilient and highly available while meeting the expected increase in demand?

A. Use AWS OpsWorks to automatically configure each new EC2 instance as it is launched. Configure the EC2 instances by using an Auto Scaling group behind an Application Load Balancer across multiple Availability Zones. ImplementAmazon DynamoDB Auto Scaling. Use Amazon Route 53 to point the application

DNS record to the Application Load Balancer.

B. Deploy a fleet of EC2 instances, doubling the current capacity, and place them behind an Application Load Balancer. Increase the Amazon DynamoDB read and write capacity units. Add an alias record that contains the Application LoadBalancer endpoint to the existing Amazon Route 53 DNS record that points to the application.

C. Configure Amazon CloudFront and have its origin point to Amazon S3 to host the web application. Implement Amazon DynamoDB Auto Scaling. Use Amazon Route 53 to point the application DNS record to the CloudFront DNS name.

D. Use AWS Elastic Beanstalk with a custom AMI including all web components. Deploy the platform by using an Auto Scaling group behind an Application Load Balancer across multiple Availability Zones. Implement Amazon DynamoDBAuto Scaling. Use Amazon Route 53 to point the application DNS record to the Elastic Beanstalk load balancer.

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

**Explanation/Reference:**

**QUESTION 17**
A DevOps Engineer is working on a project that is hosted on Amazon Linux and has failed a security review. The DevOps Manager has been asked to review the company buildspec.yaml file for an AWS CodeBuild project and provide recommendations. The buildspec.yaml file is configured as follows:

```
env:
variables:
AWS_ACCESS_KEY_ID: AKIAJF7BRFWJBA4GHXNA
AWS_SECRET_ACCESS_KEY: ORjJns3At2mIh4O4tm0+zHxZqz7cNAvMLYRehcI
AWS_DEFAULT_REGION: us-east-1
DB_PASSWORD: cuj5RptFa3va
phases:
build:
commands:
-aws s3 cp s3://db-deploy-bucket/my.cnf.template/tmp/my.cnf
-sed-i '' s/DB_PW/${DB_PASSWORD}/ /tmp/my.cnf
-aws s3 cp s3:// db-deploy-bucket/instance.key/tmp/instance.key
-chmod 600/tmp/instance.key
-scp-i /tmp/instance.key/tmp/my.cnf root@10.25.23:/etc/my.cnf
-ssh- i /tmp/instance.key root@10.25.15.23 /etc/init.d/mysqld restart
```



What changes should be recommended to comply with AWS security best practices? (Select THREE.)

A. Add a post-build command to remove the temporary files from the container before termination to ensure they cannot be seen by other CodeBuild users.
B. Update the CodeBuild project role with the necessary permissions and then remove the AWS credentials from the environment variable.
C. Store the DB_PASSWORD as a SecureString value in AWS Systems Manager Parameter Store and then remove the DB_PASSWORD from the environment variables.
D. Move the environment variables to the 'db-deploy-bucket' Amazon S3 bucket, add a prebuild stage to download, then export the variables.
E. Use AWS Systems Manager run command versus scp and ssh commands directly to the instance.
F. Scramble the environment variables using XOR followed by Base64, add a section to install, and then run XOR and Base64 to the build phase.

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

**Explanation/Reference:**

**QUESTION 18**

A Development team is building more than 40 applications. Each app is a three-tiered web application based on an ELB Application Load Balancer, Amazon EC2, and Amazon RDS. Because the applications will be used internally, the Security team wants to allow access to the 40 applications only from the corporate network and block access from external IP addresses. The corporate network reaches the internet through proxy servers. The proxy servers have 12 proxy IP addresses that are being changed one or two times per month. The Network Infrastructure team manages the proxy servers; they upload the file that contains the latest proxy IP addresses into an Amazon S3 bucket. The DevOps Engineer must build a solution to ensure that the applications are accessible from the corporate network.
Which solution achieves these requirements with MINIMAL impact to application development, MINIMAL operational effort, and the LOWEST infrastructure cost?

A. Implement an AWS Lambda function to read the list of proxy IP addresses from the S3 object and to update the ELB security groups to allow HTTPS only from the given IP addresses. Configure the S3 bucket to invoke the Lambdafunction when the object is updated. Save the IP address list to the S3 bucket when they are changed.
B. Ensure that all the applications are hosted in the same Virtual Private Cloud (VPC). Otherwise, consolidate the applications into a single VPC. Establish an AWS Direct Connect connection with an active/standby configuration. Changethe ELB security groups to allow only inbound HTTPS connections from the corporate network IP addresses.
C. Implement a Python script with the AWS SDK for Python (Boto), which downloads the S3 object that contains the proxy IP addresses, scans the ELB security groups, and updates them to allow only HTTPS inbound from the given IPaddresses. Launch an EC2 instance and store the script in the instance. Use a cron job to execute the script daily.
D. Enable ELB security groups to allow HTTPS inbound access from the Internet. Use Amazon Cognito to integrate the company's Active Directory as the identity provider. Change the 40 applications to integrate with Amazon Cognito sothat only company employees can log into the application. Save the user access logs to Amazon CloudWatch Logs to record user access activities



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

**Explanation/Reference:**

**QUESTION 19**
A company is implementing AWS CodePipeline to automate its testing process. The company wants to be notified when the execution state fails and used the following custom event pattern in Amazon CloudWatch:

```
{
  "source": [
    "aws.codepipeline"
  ],
  "detail-type": [
    "CodePipeline Action Execution State Change"
  ],
  "detail": {
    "state": [
      "FAILED"
  ],
  "type": {
    "category": ["Approval"]
      }
  }
}
```

Which type of events will match this event pattern?

A. Failed deploy and build actions across all the pipelines.
B. All rejected or failed approval actions across all the pipelines.
C. All the events across all pipelines.
D. Approval actions across all the pipelines.



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

**Explanation/Reference:**
Reference:
https://docs.aws.amazon.com/codepipeline/latest/userguide/detect-state-changes-cloudwatchevents.html

**QUESTION 20**
A company is using several AWS CloudFormation templates for deploying infrastructure as code. In most of the deployments, the company uses Amazon EC2 Auto Scaling groups. A DevOps Engineer needs to update the AMIs for the Auto Scaling group in the template if newer AMIs are available. How can these requirements be met?

A. Manage the AMI mappings in the CloudFormation template. Use Amazon CloudWatch Events for detecting new AMIs and updating the mapping in the template. Reference the map in the launch configuration resource block.
B. Use conditions in the AWS CloudFormation template to check if new AMIs are available and return the AMI ID. Reference the returned AMI ID in the launch configuration resource block.

C. Use an AWS Lambda-backed custom resource in the template to fetch the AMI IDs. Reference the returned AMI ID in the launch configuration resource block.
D. Launch an Amazon EC2 m4.small instance and run a script on it to check for new AMIs. If new AMIs are available, the script should update the launch configuration resource block with the new AMI ID.

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

**Explanation/Reference:**
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/walkthrough-customresources-lambda-lookup-amiids.html

**QUESTION 21**
A DevOps Engineer administers an application that manages video files for a video production company. The application runs on Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. Data is stored in an Amazon RDS PostgreSQL Multi-AZ DB instance, and the video files are stored in an Amazon S3 bucket. On a typical day, 50 GB of new video are added to the S3 bucket. The Engineer must implement a multi-region disaster recovery plan with the least data loss and the lowest recovery times. The current application infrastructure is already described using AWS CloudFormation. Which deployment option should the Engineer choose to meet the uptime and recovery objectives for the system?

A. Launch the application from the CloudFormation template in the second region, which sets the capacity of the Auto Scaling group to 1. Create an Amazon RDS read replica in the second region. In the second region, enable cross-regionreplication between the original S3 bucket and a new S3 bucket. To fail over, promote the read replica as master. Update the CloudFormation stack and increase the capacity of the Auto Scaling group.
B. Launch the application from the CloudFormation template in the second region, which sets the capacity of the Auto Scaling group to 1. Create a scheduled task to take daily Amazon RDS cross-region snapshots to the second region. Inthe second region, enable cross-region replication between the original S3 bucket and Amazon Glacier. In a disaster, launch a new application stack in the second region and restore the database from the most recent snapshot.
C. Launch the application from the CloudFormation template in the second region which sets the capacity of the Auto Scaling group to 1. Use Amazon CloudWatch Events to schedule a nightly task to take a snapshot of the database, copythe snapshot to the second region, and replace the DB instance in the second region from the snapshot. In the second region, enable cross-region replication between the original S3 bucket and a new S3 bucket. To fail over, increase the capacity of the Auto Scaling group.
D. Use Amazon CloudWatch Events to schedule a nightly task to take a snapshot of the database and copy the snapshot to the second region. Create an AWS Lambda function that copies each object to a new S3 bucket in the secondregion in response to S3 event notifications. In the second region, launch the application from the CloudFormation template and restore the database from the most recent snapshot.

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

**Explanation/Reference:**

**QUESTION 22**
A social networking service runs a web API that allows its partners to search public posts. Post data is stored in Amazon DynamoDB and indexed by AWS Lambda functions, with an Amazon ES domain storing the indexes and providing search functionality to the application.
The service needs to maintain full capacity during deployments and ensure that failed deployments do not cause downtime or reduced capacity, or prevent subsequent deployments. How can these requirements be met? (Select TWO )

A. Run the web application in AWS Elastic Beanstalk with the deployment policy set to All at Once. Deploy the Lambda functions, DynamoDB tables, and Amazon ES domain with an AWS CloudFormation template.
B. Deploy the web application, Lambda functions, DynamoDB tables, and Amazon ES domain in an AWS CloudFormation template. Deploy changes with an AWS CodeDeploy in-place deployment.
C. Run the web application in AWS Elastic Beanstalk with the deployment policy set to Immutable. Deploy the Lambda functions, DynamoDB tables, and Amazon ES domain with an AWS CloudFormation template.
D. Deploy the web application, Lambda functions, DynamoDB tables, and Amazon ES domain in an AWS CloudFormation template. Deploy changes with an AWS CodeDeploy blue/green deployment.
E. Run the web application in AWS Elastic Beanstalk with the deployment policy set to Rolling. Deploy the Lambda functions, DynamoDB tables, and Amazon ES domain with an AWS CloudFormation template.

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

**Explanation/Reference:**



**QUESTION 23**
A media customer has several thousand amazon EC2 instances in an AWS account. The customer is using a Slack channel for team communications and important updates. A DevOps Engineer was told to send all AWS-scheduled EC2 maintenance notifications to the company Slack channel.
Which method should the Engineer use to implement this process in the LEAST amount of steps?

A. Integrate AWS Trusted Advisor with AWS Config. Based on the AWS Config rules created, the AWS Config event can invoke an AWS Lambda function to send notifications to the Slack channel.
B. Integrate AWS Personal Health Dashboard with Amazon CloudWatch Events. Based on the CloudWatch Events created, the event can invoke an AWS Lambda function to send notifications to the Slack channel.
C. Integrate EC2 events with Amazon CloudWatch monitoring. Based on the CloudWatch Alarm created, the alarm can invoke an AWS Lambda function to send EC2 maintenance notifications to the Slack channel.
D. Integrate AWS Support with AWS CloudTrail. Based on the CloudTrail lookup event created, the event can invoke an AWS Lambda function to pass EC2 maintenance notifications to the Slack channel.

**Correct Answer:** B

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

**Explanation/Reference:**
Reference:
https://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html

**QUESTION 24**
After conducting a disaster recovery exercise, an Enterprise Architect discovers that a large team of Database and Storage Administrators need more than seven hours of manual effort to make a flagship application's database functional in a different AWS Region. The Architect also discovers that the recovered database is often missing as much as two hours of data transactions. Which solution provides improved RTO and RPO in a cross-region failover scenario?

A. Deploy an Amazon RDS Multi-AZ instance backed by a multi-region Amazon EFS. Configure the RDS option group to enable multi-region availability for native automation of cross-region recovery and continuous data replication. Createan Amazon SNS topic subscribed to RDS-impacted events to send emails to the Database Administration team when significant query Latency is detected in a single Availability Zone.
B. Use Amazon SNS topics to receive published messages from Amazon RDS availability and backup events. Use AWS Lambda for three separate functions with calls to Amazon RDS to snapshot a database instance, create a cross-region snapshot copy, and restore an instance from a snapshot. Use a scheduled Amazon CloudWatch Events rule at a frequency matching the RPO to trigger the Lambda function to snapshot a database instance. Trigger the Lambda function to create a cross-region snapshot copy when the SNS topic for backup events receives a new message. Configure the Lambda function to restore an instance from a snapshot to trigger sending new messages published to the availability SNS topic.
C. Create a scheduled Amazon CloudWatch Events rule to make a call to Amazon RDS to create a snapshot from a database instance and specify a frequency to match the RPO. Create an AWS Step Functions task to call Amazon RDS toperform a cross-region snapshot copy into the failover region, and configure the state machine to execute the task when the RDS snapshot create state is complete. Create an SNS topic subscribed to RDS availability events, and push these messages to an Amazon SQS queue located in the failover region. Configure an Auto Scaling group of worker nodes to poll the queue for new messages and make a call to Amazon RDS to restore a database from a snapshot after a checksum on the cross-region copied snapshot returns valid.
D. Use Amazon RDS scheduled instance lifecycle events to create a snapshot and specify a frequency to match the RPO. Use Amazon RDS scheduled instance lifecycle event configuration to perform a cross-region snapshot copy into thefailover region upon SnapshotCreateComplete events. Configure Amazon CloudWatch to alert when the CloudWatch RDS namespace CPUUtilization metric for the database instance falls to 0% and make a call to Amazon RDS to restore the database snapshot in the failover region.

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

**Explanation/Reference:**

**QUESTION 25**
A company has deployed several applications globally. Recently, Security Auditors found that few Amazon EC2 instances were launched without Amazon EBS disk encryption. The Auditors have requested a report detailing all EBS volumes that were not encrypted in multiple AWS accounts and regions. They also want

to be notified whenever this occurs in future. How can this be automated with the LEAST amount of operational overhead?

A. Create an AWS Lambda function to set up an AWS Config rule on all the target accounts. Use AWS Config aggregators to collect data from multiple accounts and regions. Export the aggregated report to an Amazon S3 bucket and useAmazon SNS to deliver the notifications.
B. Set up AWS CloudTrail to deliver all events to an Amazon S3 bucket in a centralized account. Use the S3 event notification feature to invoke an AWS Lambda function to parse AWS CloudTrail logs whenever logs are delivered to theS3 bucket. Publish the output to an Amazon SNS topic using the same Lambda function.
C. Create an AWS CloudFormation template that adds an AWS Config managed rule for EBS encryption. Use a CloudFormation stack set to deploy the template across all accounts and regions. Store consolidated evaluation results fromconfig rules in Amazon S3. Send a notification using Amazon SNS when non-compliant resources are detected.
D. Using AWS CLI, run a script periodically that invokes the aws ec2 describe-volumes query with a JMESPATH query filter. Then, write the output to an Amazon S3 bucket. Set up an S3 event notification to send events using AmazonSNS when new data is written to the S3 bucket.

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

**Explanation/Reference:**



**QUESTION 26**
A DevOps Engineer has a single Amazon Dynamo DB table that receives shipping orders and tracks inventory. The Engineer has three AWS Lambda functions reading from a DymamoDB stream on that table. The Lambda functions perform various functions such as doing an item count, moving items to Amazon Kinesis Data Firehose, monitoring inventory levels, and creating vendor orders when parts are low.
While reviewing logs, the Engineer notices the Lambda functions occasionally fail under increased load, receiving a stream throttling error.
Which is the MOST cost-effective solution that requires the LEAST amount of operational management?

A. Use AWS Glue integration to ingest the DynamoDB stream, then migrate the Lambda code to an AWS Fargate task.
B. Use Amazon Kinesis streams instead of Dynamo DB streams, then use Kinesis analytics to trigger the Lambda functions.
C. Create a fourth Lambda function and configure it to be the only Lambda reading from the stream. Then use this Lambda function to pass the payload to the other three Lambda functions.
D. Have the Lambda functions query the table directly and disable DynamoDB streams. Then have the Lambda functions query from a global secondary index.

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

**Explanation/Reference:**

**QUESTION 27**
A government agency is storing highly confidential files in an encrypted Amazon S3 bucket. The agency has configured federated access and has allowed only a particular on-premises Active Directory user group to access this bucket. The agency wants to maintain audit records and automatically detect and revert any accidental changes administrators make to the IAM policies used for providing this restricted federated access. Which of the following options provide the FASTEST way to meet these requirements?

A. Configure an Amazon CloudWatch Events Event Bus on an AWS CloudTrail API for triggering the AWS Lambda function that detects and reverts the change.
B. Configure an AWS Config rule to detect the configuration change and execute an AWS Lambda function to revert the change.
C. Schedule an AWS Lambda function that will scan the IAM policy attached to the federated access role for detecting and reverting any changes.
D. Restrict administrators in the on-premises Active Directory from changing the IAM policies.

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

**Explanation/Reference:**

**QUESTION 28**
A healthcare provider has a hybrid architecture that includes 120 on-premises VMware servers running RedHat and 50 Amazon EC2 instances running Amazon Linux. The company is in the middle of an all-in migration to AWS and wants to implement a solution for collecting information from the on-premises virtual machines and the EC2 instances for data analysis. The information includes:
- Operating system type and version
- Data for installed applications
- Network configuration information, such as MAC and IP addresses- Amazon EC2 instance AMI ID and IAM profile
How can these requirements be met with the LEAST amount of administration?

A. Write a shell script to run as a cron job on EC2 instances to collect and push the data to Amazon S3. For on-premises resources, use VMware vSphere to collect the data and write it into a file gateway for storing the data in S3. Finally,use Amazon Athena on the S3 bucket for analytics.
B. Use a script on the on-premises virtual machines as well as the EC2 instances to gather and push the data into Amazon S3, and then use Amazon Athena for analytics.
C. Install AWS Systems Manager agents on both the on-premises virtual machines and the EC2 instances. Enable inventory collection and configure resource data sync to an Amazon S3 bucket to analyze the data with Amazon Athena.
D. Use AWS Application Discovery Service for deploying Agentless Discovery Connector in the VMware environment and Discovery Agents on the EC2 instances for collecting the data. Then use the AWS Migration Hub Dashboard for analytics.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 29**
A company must ensure consistent behavior of an application running on Amazon Linux in its corporate ecosystem before moving into AWS. The company has an existing automated server build system using VMware. The goal is to demonstrate the functionality of the application and its prerequisites on the new target operating system.
The DevOps Engineer needs to use the existing corporate server pipeline and virtualization software to create a server image. The server image will be tested on-premises to resemble the build on Amazon EC2 as closely as possible. How can this be accomplished?

A. Download and integrate the latest ISO of CentOS 7 and execute the application deployment on the resulting server.
B. Launch an Amazon Linux AMI using an AWS OpsWorks deployment agent onto the on-premises infrastructure, then execute the application deployment.
C. Build an EC2 instance with the latest Amazon Linux operating system, and use the AWS Import/Export service to export the EC2 image to a VMware ISO in Amazon S3. Then import the resulting ISO onto the on-premises system.
D. Download and integrate the latest ISO of Amazon Linux 2 and execute the application deployment on the resulting server. Confirm that operating system testing results are consistent with EC2 operating system behavior.

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



**Explanation/Reference:**
Reference:
https://aws.amazon.com/blogs/aws/opsworks-on-prem-and-existing-instances/

**QUESTION 30**
A Development team is adding a new country to an e-commerce application. This addition requires that new application features be added to the shipping component of the application. The team has not decided if all new features should be added, as some will take approximately six weeks to build. While the final decision on the shipping component features is being made, other team members are continuing to work on other features of the application. Based on this situation, how should the application feature deployments be managed?

A. Add the code updates as commits to the release branch. The team can delay the deployment until all features are ready.
B. Add the code updates as commits to a feature branch. Merge the commits to a release branch as features are ready.
C. Add the code updates as a single commit when a feature is ready. Tag this commit with "new-country."
D. Create a new repository named "new-country". Commit all the code changes to the new repository.

**Correct Answer:** B

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

**Explanation/Reference:**

**QUESTION 31**
A DevOps Engineer is asked to implement a strategy for deploying updates to a web application with zero downtime. The application infrastructure is defined in AWS CloudFormation and is made up of an Amazon Route 53 record, an Application Load Balancer, Amazon EC2 instances in an EC2 Auto Scaling group, and Amazon DynamoDB tables. To avoid downtime, there must be an active instance serving the application at all times. Which strategies will ensure the deployment happens with zero downtime? (Select TWO.)

A. In the CloudFormation template, modify the AWS::AutoScaling::AutoscalingGroup resource and add an UpdatePolicy attribute to define the required elements for a deployment with zero downtime.
B. In the CloudFormation template, modify the AWS:: AutoScaling::DeploymentUpdates resource and add an UpdatePolicy attribute to define the required elements for a deployment with zero downtime.
C. Add a new Application Load Balancer and Auto Scaling group to the CloudFormation template. Deploy new changes to the inactive Auto Scaling group. Use Route 53 to change the active Application Load Balancer.
D. Add a new Application Load Balancer and Auto Scaling group to the CloudFormation template. Modify the AWS::AutoScaling::AutoScalingGroup resource and add an UpdatePolicy attribute to perform rolling updates.
E. In the CloudFormation template, modify the UpdatePolicy attribute for the CloudFormation stack and specify the Auto Scaling group that will be updated. Configure MinSuccessfulInstancesPercent and PauseTime to ensure thedeployment happens with zero downtime.

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

**Explanation/Reference:**

**QUESTION 32**
A DevOps Engineer must create a Linux AMI in an automated fashion. The newly created AMI identification must be stored in a location where other build pipelines can access the new identification programmatically What is the MOST cost-effective way to do this?

A. Build a pipeline in AWS CodePipeline to download and save the latest operating system Open Virtualization Format (OVF) image to an Amazon S3 bucket, then customize the image using the guestfish utility. Use the virtual machine(VM) import command to convert the OVF to an AMI, and store the AMI identification output as an AWS Systems Manager parameter.
B. Create an AWS Systems Manager automation document with values instructing how the image should be created. Then build a pipeline in AWS CodePipeline to execute the automation document to build the AMI when triggered. Storethe AMI identification output as a Systems Manager parameter.

C. Build a pipeline in AWS CodePipeline to take a snapshot of an Amazon EC2 instance running the latest version of the application. Then start a new EC2 instance from the snapshot and update the running instance using an AWS Lambdafunction. Take a snapshot of the updated instance, then convert it to an AMI. Store the AMI identification output in an Amazon DynamoDB table.

D. Launch an Amazon EC2 instance and install Packer. Then configure a Packer build with values defining how the image should be created. Build a Jenkins pipeline to invoke the Packer build when triggered to build an AMI. Store the AMIidentification output in an Amazon DynamoDB table.

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

**Explanation/Reference:**

**QUESTION 33**
An application is being deployed with two Amazon EC2 Auto Scaling groups, each configured with an Application Load Balancer. The application is deployed to one of the Auto Scaling groups and an Amazon Route 53 alias record is pointed to the Application Load Balancer of the last deployed Auto Scaling group. Deployments alternate between the two Auto Scaling groups.
Home security devices are making requests into the application. The Development team notes that new requests are coming into the old stack days after the deployment. The issue is caused by devices that are not observing the Time to Live (TTL) setting on the Amazon Route 53 alias record.
What steps should the DevOps Engineer take to address the issue with requests coming to the old stacks, while creating minimal additional resources?



A. Create a fleet of Amazon EC2 instances running HAProxy behind an Application Load Balancer. The HAProxy instances will proxy the requests to one of the existing Auto Scaling groups. After a deployment the HAProxy instances areupdated to send requests to the newly deployed Auto Scaling group.

B. Reduce the application to one Application Load Balancer. Create two target groups named Blue and Green. Create a rule on the Application Load Balancer pointed to a single target group. Add logic to the deployment to update theApplication Load Balancer rule to the target group of the newly deployed Auto Scaling group.

C. Move the application to an AWS Elastic Beanstalk application with two environments. Perform new deployments on the non-live environment. After a deployment, perform an Elastic Beanstalk CNAME swap to make the newly deployedenvironment the live environment.

D. Create an Amazon CloudFront distribution. Set the two existing Application Load Balancers as origins on the distribution. After a deployment, update the CloudFront distribution behavior to send requests to the newly deployed AutoScaling group.

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

**Explanation/Reference:**

**QUESTION 34**
A company has microservices running in AWS Lambda that read data from Amazon DynamoDB. The Lambda code is manually deployed by Developers after

successful testing. The company now needs the tests and deployments be automated and run in the cloud. Additionally, traffic to the new versions of each microservice should be incrementally shifted over time after deployment. What solution meets all the requirements, ensuring the MOST developer velocity?

A. Create an AWS CodePipeline configuration and set up a post-commit hook to trigger the pipeline after tests have passed. Use AWS CodeDeploy and create a Canary deployment configuration that specifies the percentage of traffic andinterval.
B. Create an AWS CodeBuild configuration that triggers when the test code is pushed. Use AWS CloudFormation to trigger an AWS CodePipeline configuration that deploys the new Lambda versions and specifies the traffic shiftpercentage and interval.
C. Create an AWS CodePipeline configuration and set up the source code step to trigger when code is pushed. Set up the build step to use AWS CodeBuild to run the tests. Set up an AWS CodeDeploy configuration to deploy, then selectthe CodeDeployDefault.LambdaLinear10PercentEvery3Minutes option.
D. Use the AWS CLI to set up a post-commit hook that uploads the code to an Amazon S3 bucket after tests have passed. Set up an S3 event trigger that runs a Lambda function that deploys the new version. Use an interval in the Lambdafunction to deploy the code over time at the required percentage.

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

**Explanation/Reference:**

**QUESTION 35**
A company is using an AWS CloudFormation template to deploy web applications. The template requires that manual changes be made for each of the three major environments: production, staging, and development. The current sprint includes the new implementation and configuration of AWS CodePipeline for automated deployments.
What changes should the DevOps Engineer make to ensure that the CloudFormation template is reusable across multiple pipelines?

A. Use a CloudFormation custom resource to query the status of the CodePipeline to determine which environment is launched. Dynamically alter the launch configuration of the Amazon EC2 instances.
B. Set up a CodePipeline pipeline for each environment to use input parameters. Use CloudFormation mappings to switch associated UserData for the Amazon EC2 instances to match the environment being launched.
C. Set up a CodePipeline pipeline that has multiple stages, one for each development environment. Use AWS Lambda functions to trigger CloudFormation deployments to dynamically alter the UserData of the Amazon EC2 instanceslaunched in each environment.
D. Use CloudFormation input parameters to dynamically alter the LaunchConfiguration and UserData sections of each Amazon EC2 instance every time the CloudFormation stack is updated.

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

**Explanation/Reference:**

**QUESTION 36**
An application runs on Amazon EC2 instances behind an Application Load Balancer. Amazon RDS MySOL is used on the backend. The instances run in an Auto Scaling group across multiple Availability Zones. The Application Load Balancer health check ensures the web servers are operating and able to make read/write SQL connections. Amazon Route 53 provides DNS functionality with a record pointing to the Application Load Balancer. A new policy requires a geographically isolated disaster recovery site with an RTO of 4 hours and an RPO of 15 minutes. Which disaster recovery strategy will require the LEAST amount of changes to the application stack?

A. Launch a replica stack of everything except RDS in a different Availability Zone. Create an RDS read-only replica in a new Availability Zone and configure the new stack to point to the local RDS instance. Add the new stack to the Route53 record set with a failover routing policy.
B. Launch a replica stack of everything except RDS in a different region. Create an RDS read-only replica in a new region and configure the new stack to point to the local RDS instance. Add the new stack to the Route 53 record set with alatency routing policy.
C. Launch a replica stack of everything except RDS in a different region. Upon failure, copy the snapshot over from the primary region to the disaster recovery region. Adjust the Amazon Route 53 record set to point to the disaster recoveryregion's Application Load Balancer.
D. Launch a replica stack of everything except RDS in a different region. Create an RDS read-only replica in a new region and configure the new stack to point to the local RDS instance. Add the new stack to the Amazon Route 53 recordset with a failover routing policy.

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



**Explanation/Reference:**

**QUESTION 37**
A company wants to use Amazon DynamoDB for maintaining metadata on its forums. See the sample data set in the image below.

**Thread**

| ForumName | Subject | LastPostDateTime | Thread |
|---|---|---|---|
| "S3" | "aaa" | "2015-03-15:17:24:31" | 12 |
| "S3" | "bbb" | "2015-01-22:23:18:01" | 3 |
| "S3" | "ccc" | "2015-02-31:13:14:21" | 4 |
| "S3" | "ddd" | "2015-01-03:09:21:11" | 9 |
| "EC2" | "yyy" | "2015-02-12:11:07:56" | 18 |
| "EC2" | "zzz" | "2015-01-18:07:33:42" | 0 |
| "RDS" | "rrr" | "2015-01-19:01:13:24" | 3 |
| "RDS" | "sss" | "2015-03-11:06:53:00" | 11 |
| "RDS" | "ttt" | "2015-10-22:12:19:44" | 5 |



A DevOps Engineer is required to define the table schema with the partition key, the sort key, the local secondary index, projected attributes, and fetch operations. The schema should support the following example searches using the least provisioned read capacity units to minimize cost.
-Search within ForumName for items where the subject starts with 'a'.
-Search forums within the given LastPostDateTime time frame.
-Return the thread value where LastPostDateTime is within the last three months.
Which schema meets the requirements?

A. Use Subject as the primary key and ForumName as the sort key. Have LSI with LastPostDateTime as the sort key and fetch operations for thread.
B. Use ForumName as the primary key and Subject as the sort key. Have LSI with LastPostDateTime as the sort key and the projected attribute thread.
C. Use ForumName as the primary key and Subject as the sort key. Have LSI with Thread as the sort key and the projected attribute LastPostDateTime.
D. Use Subject as the primary key and ForumName as the sort key. Have LSI with Thread as the sort key and fetch operations for LastPostDateTime.

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

**Explanation/Reference:**

**QUESTION 38**
A company used AWS CloudFormation to deploy a three-tier web application that stores data in an Amazon RDS MySOL Multi-AZ DB instance. A DevOps Engineer must upgrade the RDS instance to the latest major version of MySQL while incurring minimal downtime.
How should the Engineer upgrade the instance while minimizing downtime?

A. Update the EngineVersion property of the AWS::RDS:: DBInstance resource type in the CloudFormation template to the latest desired version. Launch a second stack and make the new RDS instance a read replica.
B. Update the DBEngineVersion property of the AWS: : RDS : :DBInstance resource type in the CloudFormation template to the latest desired version. Perform an Update Stack operation. Create a new RDS Read Replicas resource withthe same properties as the instance to be upgraded. Perform a second Update Stack operation.
C. Update the DBEngineVersion property of the AWS: :RDS: :DB:Instance resource type in the CloudFormation template to the latest desired version. Create a new RDS Read Replicas resource with the same properties as the instance tobe upgraded. Perform an Update Stack operation.
D. Update the EngineVersion property of the AWS :: RDS :: DBInstance resource type in the CloudFormation template to the latest version, and perform an Update Stack operation.

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



**Explanation/Reference:**

**QUESTION 39**
A retail company has adopted AWS OpsWorks for managing its deployments. In the last three months, the company has discovered that some production instances have been restarting without reason. Upon inspection of the AWS CloudTrail logs, a DevOps Engineer determined that those instances were restarted by OpsWorks. The Engineer now wants automated email notifications whenever OpsWorks restarts an instance when the instance is deemed unhealthy or unable to communicate with the service endpoint. How can the Engineer meet this requirement?

A. Create a Chef recipe to place a cron to run a custom script within the Amazon EC2 instances that sends an email to the team by using Amazon SES if the OpsWorks agent detects an instance failure.
B. Create an Amazon SNS topic and create a subscription for this topic that contains the destination email address. Create an Amazon CloudWatch rule: specify aws . opsworks as a source and specify auto-healing in the initiated_bydetails. Use the SNS topic as a target.
C. Create an Amazon SNS topic and create a subscription for this topic that contains the destination email address. Create an Amazon CloudWatch rule specify aws. opsworks as a source and specify instance-replacement in theinitiated_by details. Use the SNS topic as a target.
D. Create a subscription for this topic that contains the email address. Enable instance restart notifications within the OpsWorks layer and indicate the destination

email address for the notification.

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

**Explanation/Reference:**

**QUESTION 40**
A healthcare services company is concerned about the growing costs of software licensing for an application for monitoring patient wellness. The company wants to create an audit process to ensure that the application is running exclusively on Amazon EC2 Dedicated Hosts. A DevOps Engineer must create a workflow to audit the application to ensure compliance. What steps should the Engineer take to meet this requirement with the LEAST administrative overhead?

A. Use AWS Systems Manager Configuration Compliance. Use calls to the put-compliance- items API action to scan and build a database of noncompliant EC2 instances based on their host placement configuration. Use an AmazonDynamoDB table to store these instance IDs for fast access. Generate a report through Systems Manager by calling the list-compliance- summaries API action.
B. Use custom Java code running on an EC2 instance. Set up EC2 Auto Scaling for the instance depending on the number of instances to be checked. Send the list of noncompliant EC2 instance IDs to an Amazon SQS queue. Set upanother worker instance to process instance IDs from the SQS queue and write them to Amazon DynamoDB. Use an AWS Lambda function to terminate noncompliant instance IDs obtained from the queue, and send them to an Amazon SNS email topic for distribution.
C. Use AWS Config. Identify all EC2 instances to be audited by enabling Config Recording on all Amazon EC2 resources for the region. Create a custom AWS Config rule that triggers an AWS Lambda function by using the "config-rule-change-triggered" blueprint. Modify the Lambda evaluateCompliance () function to verify host placement to return a NON_COMPLIANT result if the instance is not running on an EC2 Dedicated Host. Use the AWS Config report to address noncompliant instances.
D. Use AWS CloudTrail. Identify all EC2 instances to be audited by analyzing all calls to the EC2 RunCommand API action. Invoke an AWS Lambda function that analyzes the host placement of the instance. Store the EC2 instance ID ofnoncompliant resources in an Amazon RDS MySOL DB instance. Generate a report by querying the RDS instance and exporting the query results to a CSV text file.

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

**Explanation/Reference:**

**QUESTION 41**
According to Information Security Policy, changes to the contents of objects inside production Amazon S3 buckets that contain encrypted secrets should only be made by a trusted group of administrators. How should a DevOps Engineer create real-time, automated checks to meet this requirement?

A. Create an AWS Lambda function that is triggered by Amazon S3 data events for object changes and that also checks the IAM user's membership in an administrator's IAM role.
B. Create a periodic AWS Config rule to query Amazon S3 Logs for changes and to check the IAM user's membership in an administrator's IAM role.
C. Create a metrics filter for Amazon CloudWatch logs to check for Amazon S3 bucket-level permission changes and to check the IAM user's membership in an administrator's IAM role.
D. Create a periodic AWS Config rule to query AWS CloudTrail logs for changes to the Amazon S3 bucket-level permissions and to check the IAM user's membership in an administrator's IAM role.

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

**Explanation/Reference:**

**QUESTION 42**
A business has an application that consists of five independent AWS Lambda functions.
The DevOps Engineer has built a CI/CD pipeline using AWS CodePipeline and AWS CodeBuild that builds, tests, packages, and deploys each Lambda function in sequence. The pipeline uses an Amazon CloudWatch Events rule to ensure the pipeline execution starts as quickly as possible after a change is made to the application source code.
After working with the pipeline for a few months, the DevOps Engineer has noticed the pipeline takes too long to complete. What should the DevOps Engineer implement to BEST improve the speed of the pipeline?

A. Modify the CodeBuild projects within the pipeline to use a compute type with more available network throughput.
B. Create a custom CodeBuild execution environment that includes a symmetric multiprocessing configuration to run the builds in parallel.
C. Modify the CodePipeline configuration to execute actions for each Lambda function in parallel by specifying the same runOrder.
D. Modify each CodeBuild project to run within a VPC and use dedicated instances to increase throughput.

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

**Explanation/Reference:**

**QUESTION 43**
A company uses a complex system that consists of networking, IAM policies, and multiple three-tier applications. Requirements are still being defined for a new system, so the number of AWS components present in the final design is not known. The DevOps Engineer needs to begin defining AWS resources using AWS CloudFormation to automate and version-control the new infrastructure. What is the best practice for using CloudFormation to create new environments?

A. Manually construct the networking layer using Amazon VPC and then define all other resources using CloudFormation.
B. Create a single template to encompass all resources that are required for the system so there is only one template to version-control.
C. Create multiple separate templates for each logical part of the system, use cross-stack references in CloudFormation, and maintain several templates in version control.
D. Create many separate templates for each logical part of the system, and provide the outputs from one to the next using an Amazon EC2 instance running SDK for granular control.

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

**Explanation/Reference:**

**QUESTION 44**
A DevOps Engineer is deploying a new web application. The company chooses AWS Elastic Beanstalk for deploying and managing the web application, and Amazon RDS MySQL to handle persistent data. The company requires that new deployments have minimal impact if they fail. The application resources must be at full capacity during deployment, and rolling back a deployment must also be possible. Which deployment sequence will meet these requirements?

A. Deploy the application using Elastic Beanstalk and connect to an external RDS MySQL instance using Elastic Beanstalk environment properties. Use Elastic Beanstalk features for a blue/green deployment to deploy the new release to aseparate environment, and then swap the CNAME in the two environments to redirect traffic to the new version.
B. Deploy the application using Elastic Beanstalk, and include RDS MySQL as part of the environment. Use default Elastic Beanstalk behavior to deploy changes to the application, and let rolling updates deploy changes to the application.
C. Deploy the application using Elastic Beanstalk, and include RDS MySQL as part of the environment. Use Elastic Beanstalk immutable updates for application deployments.
D. Deploy the application using Elastic Beanstalk, and connect to an external RDS MySQL instance using Elastic Beanstalk environment properties. Use Elastic Beanstalk immutable updates for application deployments.

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

**Explanation/Reference:**

**QUESTION 45**
Am Amazon EC2 instance with no internet access is running in a Virtual Private Cloud (VPC) and needs to download an object from a restricted Amazon S3

bucket. When the DevOps Engineer tries to gain access to the object, an AccessDenied error is received.
What are the possible causes for this error? (Select THREE.)

A. The S3 bucket default encryption is enabled.
B. There is an error in the S3 bucket policy.
C. There is an error in the VPC endpoint policy.
D. The object has been moved to Amazon Glacier.
E. There is an error in the IAM role configuration.
F. S3 versioning is enabled.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/s3-403-upload-bucket/

**QUESTION 46**
An application has microservices spread across different AWS accounts and is integrated with an on-premises legacy system for some of its functionality. Because of the segmented architecture and missing logs, every time the application experiences issues, it is taking too long to gather the logs to identify the issues. A DevOps Engineer must fix the log aggregation process and provide a way to centrally analyze the logs. Which is the MOST efficient and cost-effective solution?

A. Collect system logs and application logs by using the Amazon CloudWatch Logs agent. Use the Amazon S3 API to export on-premises logs, and store the logs in an S3 bucket in a central account. Build an Amazon EMR cluster to reducethe logs and derive the root cause.
B. Collect system logs and application logs by using the Amazon CloudWatch Logs agent. Use the Amazon S3 API to import on-premises logs. Store all logs in S3 buckets in individual accounts. Use Amazon Macie to write a query tosearch for the required specific event-related data point.
C. Collect system logs and application logs using the Amazon CloudWatch Logs agent. Install the CloudWatch Logs agent on the on-premises servers. Transfer all logs from AWS to the on-premises data center. Use an AmazonElasticsearch Logstash Kibana stack to analyze logs on premises.
D. Collect system logs and application logs by using the Amazon CloudWatch Logs agent. Install a CloudWatch Logs agent for on-premises resources. Store all logs in an S3 bucket in a central account. Set up an Amazon S3 trigger and anAWS Lambda function to analyze incoming logs and automatically identify anomalies. Use Amazon Athena to run ad hoc queries on the logs in the central account.

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

**Explanation/Reference:**

**QUESTION 47**
A DevOps Engineer is building a continuous deployment pipeline for a serverless application using AWS CodePipeline and AWS CodeBuild. The source, build, and test stages have been created with the deploy stage remaining. The company wants to reduce the risk of an unsuccessful deployment by deploying to a small percentage of customers and monitoring this deployment prior to a full release to all customers. How should the deploy stage be configured to meet these requirements?

A. Use AWS CloudFormation to publish a new version on every stack update. Then set up a CodePipeline approval action for a Developer to test and approve the new version. Finally, use a CodePipeline invoke action to update an AWSLambda function to use the production alias
B. Use CodeBuild to use the AWS CLI to update the AWS Lambda function code, then publish a new version of the function and update the production alias to point to the new version of the function.
C. Use AWS CloudFormation to define the serverless application and AWS CodeDeploy to deploy the AWS Lambda functions using DeploymentPreference: Canary10Percentl5Minutes.
D. Use AWS CloudFormation to publish a new version on every stack update. Use the RoutingConfig property of the AWS : :Lambda: : Alias resource to update the traffic routing during the stack update.

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

**Explanation/Reference:**



**QUESTION 48**
A DevOps Engineer must track the health of a stateless RESTful service sitting behind a Classic Load Balancer. The deployment of new application revisions is through a Cl/CD pipeline. If the service's latency increases beyond a defined threshold, deployment should be stopped until the service has recovered. Which of the following methods allow for the QUICKEST detection time?

A. Use Amazon CloudWatch metrics provided by Elastic Load Balancing to calculate average latency. Alarm and stop deployment when latency increases beyond the defined threshold.
B. Use AWS Lambda and Elastic Load Balancing access logs to detect average latency. Alarm and stop deployment when latency increases beyond the defined threshold.
C. Use AWS CodeDeploy's MinimumHealthyHosts setting to define thresholds for rolling back deployments. If these thresholds are breached, roll back the deployment.
D. Use Metric Filters to parse application logs in Amazon CloudWatch Logs. Create a filter for latency. Alarm and stop deployment when latency increases beyond the defined threshold.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 49**
A DevOps Engineer is leading the implementation for automating patching of Windows-based workstations in a hybrid cloud environment by using AWS Systems Manager (SSM). What steps should the Engineer follow to set up Systems Manager to automate patching in this environment? (Select TWO.)

A. Create multiple IAM service roles for Systems Manager so that the ssm.amazonaws.com service can execute the AssumeRole operation on every instance. Register the role on a per-resource level to enable the creation of a servicetoken. Perform managed-instance activation with the newly created service role attached to each managed instance.
B. Create an IAM service role for Systems Manager so that the ssm.amazonaws.com service can execute the AssumeRole operation. Register the role to enable the creation of a service token. Perform managed-instance activation with thenewly created service role.
C. Using previously obtained activation codes and activation IDs, download and install the SSM Agent on the hybrid servers, and register the servers or virtual machines on the Systems Manager service. Hybrid instances will show with an"mi-" prefix in the SSM console.
D. Using previously obtained activation codes and activation IDs, download and install the SSM Agent on the hybrid servers, and register the servers or virtual machines on the Systems Manager service. Hybrid instances will show with an"i-" prefix in the SSM console as if they were provisioned as a regular Amazon EC2 instance.
E. Run AWS Config to create a list of instances that are unpatched and not compliant. Create an instance scheduler job, and through an AWS Lambda function, perform the instance patching to bring them up to compliance.



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

**Explanation/Reference:**

**QUESTION 50**
A company needs to introduce automatic DNS failover for a distributed web application to a disaster recovery or standby installation. The DevOps Engineer plans to configure Amazon Route 53 to provide DNS routing to alternate endpoint in the event of an application failure.
What steps should the Engineer take to accomplish this? (Select TWO.)

A. Create Amazon Route 53 health checks for each endpoint that cannot be entered as alias records. Ensure firewall and routing rules allow Amazon Route 53 to send requests to the endpoints that are specified in the health checks.
B. Create alias records that route traffic to AWS resources and set the value of the Evaluate Target Health option to Yes, then create all the non-alias records.
C. Create a governing Amazon Route 53 record set, set it to failover, and associate it with the primary and secondary Amazon Route 53 record sets to distribute traffic to healthy DNS entries.

D. Create an Amazon CloudWatch alarm to monitor the primary Amazon Route 53 DNS entry. Then create an associated AWS Lambda function to execute the failover API call to Route 53 to the secondary DNS entry.
E. Map the primary and secondary Amazon Route 53 record sets to an Amazon CloudFront distribution using primary and secondary origins.

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

**Explanation/Reference:**

**QUESTION 51**
A company is implementing an Amazon ECS cluster to run its workload. The company architecture will run multiple ECS services on the cluster, with an Application Load Balancer on the front end, using multiple target groups to route traffic. The Application Development team has been struggling to collect logs that must be collected and sent to an Amazon S3 bucket for near-real time analysis What must the DevOps Engineer configure in the deployment to meet these requirements? (Select THREE)

A. Install the Amazon CloudWatch Logs logging agent on the ECS instances. Change the logging driver in the ECS task definition to 'awslogs'.
B. Download the Amazon CloudWatch Logs container instance from AWS and configure it as a task. Update the application service definitions to include the logging task.
C. Use Amazon CloudWatch Events to schedule an AWS Lambda function that will run every 60 seconds running the create-export -task CloudWatch Logs command, then point the output to the logging S3 bucket.
D. Enable access logging on the Application Load Balancer, then point it directly to the S3 logging bucket.
E. Enable access logging on the target groups that are used by the ECS services, then point it directly to the S3 logging bucket.
F. Create an Amazon Kinesis Data Firehose with a destination of the S3 logging bucket, then create an Amazon CloudWatch Logs subscription filter for Kinesis.

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

**Explanation/Reference:**

**QUESTION 52**
A Development team is currently using AWS CodeDeploy to deploy an application revision to an Auto Scaling group. If the deployment process fails, it must be rolled back automatically and a notification must be sent. What is the MOST effective configuration that can satisfy all of the requirements?

A. Create Amazon CloudWatch Events rules for CodeDeploy operations. Configure a CloudWatch Events rule to send out an Amazon SNS message when the deployment fails. Configure CodeDeploy to automatically roll back when thedeployment fails.

B. Use available Amazon CloudWatch metrics for CodeDeploy to create CloudWatch alarms. Configure CloudWatch alarms to send out an Amazon SNS message when the deployment fails. Use AWS CLI to redeploy a previouslydeployed revision.
C. Configure a CodeDeploy agent to create a trigger that will send notification to Amazon SNS topics when the deployment fails. Configure CodeDeploy to automatically roll back when the deployment fails.
D. Use AWS CloudTrail to monitor API calls made by or on behalf of CodeDeploy in the AWS account. Send an Amazon SNS message when deployment fails. Use AWS CLI to redeploy a previously deployed revision.

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

**Explanation/Reference:**

**QUESTION 53**
A large enterprise is deploying a web application on AWS. 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 application stores data in an Amazon RDS Oracle DB instance and Amazon DynamoDB. There are separate environments for development, testing, and production. What is the MOST secure and flexible way to obtain password credentials during deployment?



A. Retrieve an access key from an AWS Systems Manager SecureString parameter to access AWS services. Retrieve the database credentials from a Systems Manager SecureString parameter.
B. Launch the EC2 instances with an EC2 IAM role to access AWS services. Retrieve the database credentials from AWS Secrets Manager.
C. Retrieve an access key from an AWS Systems Manager plaintext parameter to access AWS services. Retrieve the database credentials from a Systems Manager SecureString parameter.
D. Launch the EC2 instances with an EC2 IAM role to access AWS services. Store the database passwords in an encrypted config file with the application artifacts.

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

**Explanation/Reference:**

**QUESTION 54**
A DevOps Engineer is designing a deployment strategy for a web application. The application will use an Auto Scaling group to launch Amazon EC2 instances using an AMI. The same infrastructure will be deployed in multiple environments (development, test, and quality assurance). The deployment strategy should meet the following requirements:
- Minimize the startup time for the instance

- Allow the same AMI to work in multiple environments
- Store secrets for multiple environments securelyHow should this be accomplished?

A. Preconfigure the AMI using an AWS Lambda function that launches an Amazon EC2 instance, and then runs a script to install the software and create the AMI. Configure an Auto Scaling lifecycle hook to determine which environmentthe instance is launched in, and, based on that finding, run a configuration script. Save the secrets on an .ini file and store them in Amazon S3. Retrieve the secrets using a configuration script in EC2 user data.

B. Preconfigure the AMI by installing all the software using AWS Systems Manager automation and configure Auto Scaling to tag the instances at launch with their specific environment. Then use a bootstrap script in user data to read thetags and configure settings for the environment. Use the AWS Systems Manager Parameter Store to store the secrets using AWS KMS.

C. Use a standard AMI from the AWS Marketplace. Configure Auto Scaling to detect the current environment. Install the software using a script in Amazon EC2 user data. Use AWS Secrets Manager to store the credentials for allenvironments.

D. Preconfigure the AMI by installing all the software and configuration for all environments. Configure Auto Scaling to tag the instances at launch with their environment. Use the Amazon EC2 user data to trigger an AWS Lambda functionthat reads the instance ID and then reconfigures the setting for the proper environment. Use the AWS Systems Manager Parameter Store to store the secrets using AWS KMS.

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

**Explanation/Reference:**



**QUESTION 55**
A Developer is maintaining a fleet of 50 Amazon EC2 Linux servers. The servers are part of an Amazon EC2 Auto Scaling group, and also use Elastic Load Balancing for load balancing.
Occasionally, some application servers are being terminated after failing ELB HTTP health checks. The Developer would like to perform a root cause analysis on the issue, but before being able to access application logs, the server is terminated.
How can log collection be automated?

A. Use Auto Scaling lifecycle hooks to put instances in a Pending:Wait state. Create an Amazon CloudWatch Alarm for EC2 Instance Terminate Successful and trigger an AWS Lambda function that executes an SSM Run Command scriptto collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

B. Use Auto Scaling lifecycle hooks to put instances in a Terminating: Wait state. Create a Config rule for EC2 Instance-terminate Lifecycle Action and trigger a step function that executes a script to collect logs, push them to Amazon S3,and complete the lifecycle action once logs are collected.

C. Use Auto Scaling lifecycle hooks to put instances in a Terminating: Wait state. Create an Amazon CloudWatch subscription filter for EC2 Instance Terminate Successful and trigger a CloudWatch agent that executes a script to calledlogs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

D. Use Auto Scaling lifecycle hooks to put instances in a Terminating:Wait state. Create an Amazon CloudWatch Events rule for EC2 'Instance-terminate Lifecycle Action and trigger an AWS Lambda function that executes a SSM RunCommand script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

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

**Explanation/Reference:**

**QUESTION 56**
A company has a web application that uses AWS Elastic Beanstalk, Amazon S3, and Amazon DynamoDB to develop a web application. The web application has increased dramatically in popularity, resulting in unpredictable spikes in traffic. A DevOps Engineer has noted that 90% of the requests are duplicate read requests to the DynamoDB table and the images stored in an S3 bucket.

How can the Engineer improve the performance of the website?

A. Use Amazon ElastiCache for Redis to cache repeated read requests to DynamoDB and AWS Elemental MediaStore to cache images stored in S3.
B. Use Amazon ElastiCache for Memcached to cache repeated read requests to DynamoDB and Amazon EFS to cache images stored in S3.
C. Use DynamoDB Accelerator to cache repeated read requests to DynamoDB and Amazon CloudFront to cache images stored in S3.
D. Use DynamoDB Streams to cache repeated read requests to DynamoDB and API Gateway to cache images stored in S3.



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

**Explanation/Reference:**

**QUESTION 57**
A company is creating a software solution that executes a specific parallel-processing mechanism. The software can scale to tens of servers in some special scenarios. This solution uses a proprietary library that is license-based, requiring that each individual server have a single, dedicated license installed. The company has 200 licenses and is planning to run 200 server nodes concurrently at most. The company has requested the following features:
- A mechanism to automate the use of the licenses at scale.
- Creation of a dashboard to use in the future to verify which licenses are available at any moment.
What is the MOST effective way to accomplish these requirements'?

A. Upload the licenses to a private Amazon S3 bucket. Create an AWS CloudFormation template with a Mappings section for the licenses. In the template, create an Auto Scaling group to launch the servers. In the user data script, acquirean available license from the Mappings section. Create an Auto Scaling lifecycle hook, then use it to update the mapping after the instance is terminated.
B. Upload the licenses to an Amazon DynamoDB table. Create an AWS CloudFormation template that uses an Auto Scaling group to launch the servers. In the user data script, acquire an available license from the DynamoDB table. Createan Auto Scaling lifecycle hook, then use it to update the mapping after the

instance is terminated.

C. Upload the licenses to a private Amazon S3 bucket. Populate an Amazon SQS queue with the list of licenses stored in S3. Create an AWS CloudFormation template that uses an Auto Scaling group to launch the servers. In the user datascript acquire an available license from SQS. Create an Auto Scaling lifecycle hook, then use it to put the license back in SQS after the instance is terminated.

D. Upload the licenses to an Amazon DynamoDB table. Create an AWS CLI script to launch the servers by using the parameter --count, with min:max instances to launch. In the user data script, acquire an available license from theDynamoDB table. Monitor each instance and, in case of failure, replace the instance, then manually update the DynamoDB table.

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

**Explanation/Reference:**

**QUESTION 58**
A company has developed a static website hosted on an Amazon S3 bucket. The website is deployed using AWS CloudFormation. The CloudFormation template defines an S3 bucket and a custom resource that copies content into the bucket from a source location.
The company has decided that it needs to move the website to a new location, so the existing CloudFormation stack must be deleted and re-created. However, CloudFormation reports that the stack could not be deleted cleanly. What is the MOST likely cause and how can the DevOps Engineer mitigate this problem for this and future versions of the website?



A. Deletion has failed because the S3 bucket has an active website configuration. Modify the CloudFormation template to remove the Website Configuration property from the S3 bucket resource.

B. Deletion has failed because the S3 bucket is not empty. Modify the custom resource's AWS Lambda function code to recursively empty the bucket when RequestType is Delete.

C. Deletion has failed because the custom resource does not define a deletion policy. Add a DeletionPolicy property to the custom resource definition with a value of RemoveOnDeletion.

D. Deletion has failed because the S3 bucket is not empty. Modify the S3 bucket resource in the CloudFormation template to add a DeletionPolicy property with a value of Empty.

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

**Explanation/Reference:**

**QUESTION 59**
A company is deploying a new mobile game on AWS for its customers around the world. The Development team uses AWS Code services and must meet the

following requirements:
- Clients need to send/receive real-time playing data from the backend frequently and with minimal latency
- Game data must meet the data residency requirement
Which strategy can a DevOps Engineer implement to meet their needs?

A. Deploy the backend application to multiple regions. Any update to the code repository triggers a two-stage build and deployment pipeline. A successful deployment in one region invokes an AWS Lambda function to copy the buildartifacts to an Amazon S3 bucket in another region. After the artifact is copied, it triggers a deployment pipeline in the new region.
B. Deploy the backend application to multiple Availability Zones in a single region. Create an Amazon CloudFront distribution to serve the application backend to global customers. Any update to the code repository triggers a two-stagebuild-and-deployment pipeline. The pipeline deploys the backend application to all Availability Zones.
C. Deploy the backend application to multiple regions. Use AWS Direct Connect to serve the application backend to global customers. Any update to the code repository triggers a two-stage build-and-deployment pipeline in the region. Aftera successful deployment in the region, the pipeline continues to deploy the artifact to another region.
D. Deploy the backend application to multiple regions. Any update to the code repository triggers a two-stage build-and-deployment pipeline in the region. After a successful deployment in the region, the pipeline invokes the pipeline inanother region and passes the build artifact location. The pipeline uses the artifact location and deploys applications in the new region.

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



**Explanation/Reference:**
Reference:
https://docs.aws.amazon.com/codepipeline/latest/userguide/integrations-actiontype.html#integrations-invoke

**QUESTION 60**
A Development team is working on a serverless application in AWS. To quickly identify and remediate potential production issues, the team decides to roll out changes to a small number of users as a test before the full release. The DevOps Engineer must develop a solution to minimize downtime and impact.
Which of the following solutions should be used to meet the requirements? (Select TWO.)

A. Create an Application Load Balancer with two target groups. Set up the Application Load Balancer for Amazon API Gateway private integration. Associate one target group to the current version and the other target group to the new version. Configure API Gateway to route 10% of incoming traffic to the new version. As the new version becomes stable, configure API Gateway to send all traffic to the new version and detach the old version from the load balancer.
B. Create an alias for an AWS Lambda function pointing to both the current and new versions. Configure the alias to route 10% of incoming traffic to the new version. As the new version is considered stable, update the alias to route all traffic to the new version.
C. Create a failover record set in AWS Route 53 pointing to the AWS Lambda endpoints for the old and new versions. Configure Route 53 to route 10% of incoming traffic to the new version. As the new version becomes stable, update theDNS record to route all traffic to the new version.
D. Create an ELB Network Load Balancer with two target groups. Set up the Network Load Balancer for Amazon API Gateway private integration Associate one target group with the current version and the other target group with the newversion. Configure the load balancer to route 10% of incoming traffic to the new

version. As the new version becomes stable, detach the old version from the load balancer.

E. In Amazon API Gateway, create a canary release deployment by adding canary settings to the stage of a regular deployment. Configure API Gateway to route 10% of the incoming traffic to the canary release. As the canary release isconsidered stable, promote it to a production release

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

**Explanation/Reference:**

**QUESTION 61**
A company wants to implement a CI/CD pipeline for an application that is deployed on AWS. The company also has a source-code analysis tool hosted on premises that checks for security flaws. The tool has not yet been migrated to AWS and can be accessed only on-premises server. The company wants to run checks against the source code as part of the pipeline before the code is compiled. The checks take anywhere from minutes to an hour to complete.
How can a DevOps Engineer meet these requirements?

A. Use AWS CodePipeline to create a pipeline. Add an action to the pipeline to invoke an AWS Lambda function after the source stage. Have the Lambda function invoke the source-code analysis tool on premises against the source inputfrom CodePipeline. The function then waits for the execution to complete and places the output in a specified Amazon S3 location.

B. Use AWS CodePipeline to create a pipeline, then create a custom action type. Create a job worker for the on-premises server that polls CodePipeline for job requests, initiates the tests, and returns the results. Configure the pipeline to invoke the custom action after the source stage.

C. Use AWS CodePipeline to create a pipeline. Add a step after the source stage to make an HTTPS request to the on-premises hosted web service that invokes a test with the source code analysis tool. When the analysis is complete, theweb service sends the results back by putting the results in an Amazon S3 output location provided by CodePipeline.

D. Use AWS CodePipeline to create a pipeline. Create a shell script that copies the input source code to a location on premises. Invoke the source code analysis tool and return the results to CodePipeline. Invoke the shell script by adding acustom script action after the source stage.

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

**Explanation/Reference:**

**QUESTION 62**
A company is adopting AWS CodeDeploy to automate its application deployments for a Java-Apache Tomcat application with an Apache webserver. The Development team started with a proof of concept, created a deployment group for a developer environment, and performed functional tests within the application. After completion, the team will create additional deployment groups for staging and production
The current log level is configured within the Apache settings, but the team wants to change this configuration dynamically when the deployment occurs, so that

they can set different log level configurations depending on the deployment group without having a different application revision for each group.
How can these requirements be met with the LEAST management overhead and without requiring different script versions for each deployment group?

A. Tag the Amazon EC2 instances depending on the deployment group. Then place a script into the application revision that calls the metadata service and the EC2 API to identify which deployment group the instance is part of. Use thisinformation to configure the log level settings. Reference the script as part of the Afterinstall lifecycle hook in the appspec.yml file.
B. Create a script that uses the CodeDeploy environment variable DEPLOYMENT_GROUP_NAME to identify which deployment group the instances is part of. Use this information to configure the log level settings. Reference this script aspart of the BeforeInstall lifecycle hook in the appspec.yml file
C. Create a CodeDeploy custom environment variable for each environment. Then place a script into the application revision that checks this environment variable to identify which deployment group the instance is part of. Use thisinformation to configure the log level settings. Reference this script as part of the ValidateService lifecycle hook in the appspec.yml file.
D. Create a script that uses the CodeDeploy environment variable DEPLOYMENT_GROUP_ID to identify which deployment group the instance is part of to configure the log level settings. Reference this script as part of the Install lifecyclehook in the appspec.yml file.

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

**Explanation/Reference:**



**QUESTION 63**
A company has an application that has predictable peak traffic times. The company wants the application instances to scale up only during the peak times. The application stores state in Amazon DynamoDB. The application environment uses a standard Node.js application stack and custom Chef recipes stored in a private Git repository.
Which solution is MOST cost-effective and requires the LEAST amount of management overhead when performing rolling updates of the application environment?

A. Create a custom AMI with the Node.js environment and application stack using Chef recipes. Use the AMI in an Auto Scaling group and set up scheduled scaling for the required times, then set up an Amazon EC2 IAM role that providespermission to access DynamoDB.
B. Create a Docker file that uses the Chef recipes for the application environment based on an official Node.js Docker image. Create an Amazon ECS cluster and a service for the application environment, then create a task based on thisDocker image. Use scheduled scaling to scale the containers at the appropriate times and attach a task-level IAM role that provides permission to access DynamoDB.
C. Configure AWS OpsWorks stacks and use custom Chef cookbooks. Add the Git repository information where the custom recipes are stored, and add a layer in OpsWorks for the Node.js application server. Then configure the customrecipe to deploy the application in the deploy step. Configure time-based instances and attach an Amazon EC2 IAM role that provides permission to access DynamoDB.
D. Configure AWS OpsWorks stacks and push the custom recipes to an Amazon S3 bucket and configure custom recipes to point to the S3 bucket. Then add an application layer type for a standard Node.js application server and configurethe custom recipe to deploy the application in the deploy step from the S3 bucket. Configure time-based instances and attach an Amazon EC2 IAM role that provides permission to access DynamoDB.

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

**Explanation/Reference:**

**QUESTION 64**
The Development team at an online retailer has moved to Business support and want to take advantage of the AWS Health Dashboard and the AWS Health API to automate remediation actions for issues with the health of AWS resources. The first use case is to respond to AWS detecting an IAM access key that is listed on a public code repository site. The automated response will be to delete the IAM access key and send a notification to the Security team.
How should this be achieved?

A. Create an AWS Lambda function to delete the IAM access key. Send AWS CloudTrail logs to AWS CloudWatch logs. Create a CloudWatch Logs metric filter for the AWS_RISK_CREDENTIALS_EXPOSED event with two actions: first,run the Lambda function; second, use Amazon SNS to send a notification to the Security team.
B. Create an AWS Lambda function to delete the IAM access key. Create an AWS Config rule for changes to aws.health and the AWS_RISK_CREDENTIALS_EXPOSED event with two actions: first, run the Lambda function; second, useAmazon SNS to send a notification to the Security team.
C. Use AWS Step Functions to create a function to delete the IAM access key, and then use Amazon SNS to send a notification to the Security team. Create an AWS Personal Health Dashboard rule for theAWS_RISK_CREDENTIALS_EXPOSED event; set the target of the Personal Health Dashboard rule to Step Functions.
D. Use AWS Step Functions to create a function to delete the IAM access key, and then use Amazon SNS to send a notification to the Security team. Create an Amazon CloudWatch Events rule with an aws.health event source and theAWS_RISK_CREDENTIALS_EXPOSED event, set the target of the CloudWatch Events rule to Step Functions.

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

**Explanation/Reference:**

**QUESTION 65**
The Security team depends on AWS CloudTrail to detect sensitive security issues in the company's AWS account. The DevOps Engineer needs a solution to auto-remediate CloudTrail being turned off in an AWS account.
What solution ensures the LEAST amount of downtime for the CloudTrail log deliveries?

A. Create an Amazon CloudWatch Events rule for the CloudTrail StopLogging event. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on the ARN of the resource in which StopLogging was called. Add theLambda function ARN as a target to the CloudWatch Events rule.

B. Deploy the AWS-managed CloudTrail-enabled AWS Config rule, set with a periodic interval of 1 hour. Create an Amazon CloudWatch Events rule for AWS Config rules compliance change. Create an AWS Lambda function that uses theAWS SDK to call StartLogging on the ARN of the resource in which StopLogging was called. Add the Lambda function ARN as a target to the CloudWatch Events rule.

C. Create an Amazon CloudWatch Events rule for a scheduled event every 5 minutes. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on a CloudTrail trail in the AWS account. Add the Lambda function ARN as a target to the CloudWatch Events rule.

D. Launch a t2.nano instance with a script running every 5 minutes that uses the AWS SDK to query CloudTrail in the current account. If the CloudTrail trail is disabled, have the script re-enable the trail.

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

**Explanation/Reference:**

**QUESTION 66**
A DevOps Engineer has been asked by the Security team to ensure that AWS CloudTrail files are not tampered with after being created. Currently, there is a process with multiple trails, using AWS IAM to restrict access to specific trails. The Security team wants to ensure they can trace the integrity of each file and make sure there has been no tampering.
Which option will require the LEAST effort to implement and ensure the legitimacy of the file while allowing the Security team to prove the authenticity of the logs?



A. Create an Amazon CloudWatch Events rule that triggers an AWS Lambda function when a new file is delivered. Configure the Lambda function to perform an MD5 hash check on the file, store the name and location of the file, and postthe returned hash to an Amazon DynamoDB table. The Security team can use the values stored in DynamoDB to verify the file authenticity.

B. Enable the CloudTrail file integrity feature on an Amazon S3 bucket. Create an IAM policy that grants the Security team access to the file integrity logs stored in the S3 bucket.

C. Enable the CloudTrail file integrity feature on the trail. Use the digest file created by CloudTrail to verify the integrity of the delivered CloudTrail files.

D. Create an AWS Lambda function that is triggered each time a new file is delivered to the CloudTrail bucket. Configure the Lambda function to execute an MD5 hash check on the file, and store the result on a tag in an Amazon S3 object.The Security team can use the information on the tag to verify the integrity of the file.

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

**Explanation/Reference:**

**QUESTION 67**

A company is building a web and mobile application that uses a serverless architecture powered by AWS Lambda and Amazon API Gateway. The company wants to fully automate the backend Lambda deployment based on code that is pushed to the appropriate environment branch in an AWS CodeCommit repository.
The deployment must have the following:
Separate environment pipelines for testing and production.
Automatic deployment that occurs for test environments only.
Which steps should be taken to meet these requirements?

A. Configure a new AWS CodePipeline service. Create a CodeCommit repository for each environment. Set up CodePipeline to retrieve the source code from the appropriate repository. Set up a deployment step to deploy the Lambdafunctions with AWS CloudFormation.
B. Create two AWS CodePipeline configurations for test and production environments. Configure the production pipeline to have a manual approval step. Create a CodeCommit repository for each environment. Set up each CodePipeline toretrieve the source code from the appropriate repository. Set up the deployment step to deploy the Lambda functions with AWS CloudFormation.
C. Create two AWS CodePipeline configurations for test and production environments. Configure the production pipeline to have a manual approval step. Create one CodeCommit repository with a branch for each environment. Set up eachCodePipeline to retrieve the source code from the appropriate branch in the repository. Set up the deployment step to deploy the Lambda functions with AWS CloudFormation.
D. Create an AWS CodeBuild configuration for test and production environments. Configure the production pipeline to have a manual approval step. Create one CodeCommit repository with a branch for each environment. Push the Lambdafunction code to an Amazon S3 bucket. Set up the deployment step to deploy the Lambda functions from the S3 bucket.



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

**Explanation/Reference:**

**QUESTION 68**
A company is using AWS for an application. The Development team must automate its deployments. The team has set up an AWS CodePipeline to deploy the application to Amazon EC2 instances by using AWS CodeDeploy after it has been built using the AWS CodeBuild service.
The team would like to add automated testing to the pipeline to confirm that the application is healthy before deploying it to the next stage of the pipeline using the same code. The team requires a manual approval action before the application is deployed, even if the test is successful. The testing and approval must be accomplished at the lowest costs, using the simplest management solution.
Which solution will meet these requirements?

A. Add a manual approval action after the last deploy action of the pipeline. Use Amazon SNS to inform the team of the stage being triggered. Next, add a test action using CodeBuild to do the required tests. At the end of the pipeline, add adeploy action to deploy the application to the next stage.
B. Add a test action after the last deploy action of the pipeline. Configure the action to use CodeBuild to perform the required tests. If these tests are successful, mark the action as successful. Add a manual approval action that usesAmazon SNS to notify the team, and add a deploy action to deploy the application to the next stage.

C. Create a new pipeline that uses a source action that gets the code from the same repository as the first pipeline. Add a deploy action to deploy the code to a test environment. Use a test action using AWS Lambda to test the deployment.Add a manual approval action by using Amazon SNS to notify the team, and add a deploy action to deploy the application to the next stage.

D. Add a test action after the last deployment action. Use a Jenkins server on Amazon EC2 to do the required tests and mark the action as successful if the tests pass. Create a manual approval action that uses Amazon SQS to notify theteam and add a deploy action to deploy the application to the next stage.

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

**Explanation/Reference:**

**QUESTION 69**
A company is building a solution for storing files containing Personally Identifiable Information (PII) on AWS.
Requirements state:
All data must be encrypted at rest and in transit.
All data must be replicated in at least two locations that are at least 500 miles apart.
Which solution meets these requirements?

A. Create primary and secondary Amazon S3 buckets in two separate Availability Zones that are at least 500 miles apart. Use a bucket policy to enforce access to the buckets only through HTTPS. Use a bucket policy to enforce Amazon S3SSE-C on all objects uploaded to the bucket. Configure cross-region replication between the two buckets.

B. Create primary and secondary Amazon S3 buckets in two separate AWS Regions that are at least 500 miles apart. Use a bucket policy to enforce access to the buckets only through HTTPS. Use a bucket policy to enforce S3-ManagedKeys (SSE-S3) on all objects uploaded to the bucket. Configure cross-region replication between the two buckets.

C. Create primary and secondary Amazon S3 buckets in two separate AWS Regions that are at least 500 miles apart. Use an IAM role to enforce access to the buckets only through HTTPS. Use a bucket policy to enforce Amazon S3-Managed Keys (SSE-S3) on all objects uploaded to the bucket. Configure cross-region replication between the two buckets.

D. Create primary and secondary Amazon S3 buckets in two separate Availability Zones that are at least 500 miles apart. Use a bucket policy to enforce access to the buckets only through HTTPS. Use a bucket policy to enforce AWS KMSencryption on all objects uploaded to the bucket. Configure cross-region replication between the two buckets. Create a KMS Customer Master Key (CMK) in the primary region for encrypting objects.

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

**Explanation/Reference:**

**QUESTION 70**
A company is using AWS CodeDeploy to automate software deployment. The deployment must meet these requirements:

- A number of instances must be available to serve traffic during the deployment. Traffic must be balanced across those instances, and the instances must automatically heal in the event of failure.
- A new fleet of instances must be launched for deploying a new revision automatically, with no manual provisioning.
- Traffic must be rerouted to the new environment to half of the new instances at a time. The deployment should succeed if traffic is rerouted to at least half of the instances; otherwise, it should fail.
- Before routing traffic to the new fleet of instances, the temporary files generated during the deployment process must be deleted.
- At the end of a successful deployment, the original instances in the deployment group must be deleted immediately to reduce costs.

How can a DevOps Engineer meet these requirements?

A. Use an Application Load Balancer and an in-place deployment. Associate the Auto Scaling group with the deployment group. Use the Automatically copy Auto Scaling group option, and use CodeDeployDefault.OneAtAtime as the deployment configuration. Instruct AWS CodeDeploy to terminate the original instances in the deployment group, and use the AllowTraffic hook within appspec.yml to delete the temporary files.
B. Use an Application Load Balancer and a blue/green deployment. Associate the Auto Scaling group and the Application Load Balancer target group with the deployment group. Use the Automatically copy Auto Scaling group option, create a custom deployment configuration with minimum healthy hosts defined as 50%, and assign the configuration to the deployment group. Instruct AWS CodeDeploy to terminate the original instances in the deployment group, and use the BeforeBlock Traffic hook within appspec.yml to delete the temporary files.
C. Use an Application Load Balancer and a blue/green deployment. Associate the Auto Scaling group and the Application Load Balancer target group with the deployment group. Use the Automatically copy Auto Scaling group option, and use CodeDeployDefault HalfAtAtime as the deployment configuration. Instruct AWS CodeDeploy to terminate the original isntances in the deployment group, and use the BeforeAllowTraffic hook within appspec.yml to delete the temporary files.
D. Use an Application Load Balancer and an in-place deployment. Associate the Auto Scaling group and Application Load Balancer target group with the deployment group. Use the Automatically copy Auto Scaling group option, and use CodeDeployDefault AllatOnce as a deployment configuration. Instruct AWS CodeDeploy to terminate the original instances in the deployment group, and use the BlockTraffic hook within appspec.yml to delete the temporary files.

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

**Explanation/Reference:**
Reference:
https://docs.aws.amazon.com/codedeploy/latest/APIReference/API_BlueGreenDeploymentConfig uration.html

**QUESTION 71**
A DevOps Engineer is working with an application deployed to 12 Amazon EC2 instances across 3 Availability Zones. New instances can be started from an AMI image. On a typical day, each EC2 instance has 30% utilization during business hours and 10% utilization after business hours. The CPU utilization has an immediate spike in the first few minutes of business hours. Other increases in CPU utilization rise gradually.

The Engineer has been asked to reduce costs while retaining the same or higher reliability.
Which solution meets these requirements?

A. Create two Amazon CloudWatch Events rules with schedules before and after business hours begin and end. Create two AWS Lambda functions, one invoked by each rule. The first function should stop nine instances after businesshours end, the second function should restart the nine instances before the business day begins.
B. Create an Amazon EC2 Auto Scaling group using the AMI image, with a scaling action based on the Auto Scaling group's CPU Utilization average with a target of 75%. Create a scheduled action for the group to adjust the minimumnumber of instances to three after business hours end and reset to six before business hours begin.
C. Create two Amazon CloudWatch Events rules with schedules before and after business hours begin and end. Create an AWS CloudFormation stack, which creates an EC2 Auto Scaling group, with a parameter for the number ofinstances. Invoke the stack from each rule, passing a parameter value of three in the morning, and six in the evening.
D. Create an EC2 Auto Scaling group using the AMI image, with a scaling action based on the Auto Scaling group's CPU Utilization average with a target of 75%. Create a scheduled action to terminate nine instances each evening after theclose of business.

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

**Explanation/Reference:**



**QUESTION 72**
A DevOps Engineer must improve the monitoring of a Finance team payments microservice that handles transactions for an e-commerce platform. The microservice runs on multiple Amazon EC2 instances. The Finance team would like to know the number of payments per minute, and the team would like to be notified when this metric falls below a specified threshold.
How can this be cost-effectively automated?

A. Have the Development team log successful transactions to an application log. Set up Logstash on each instance, which sends logs to an Amazon ES cluster. Create a Kibana dashboard for the Finance team that graphs the metric.
B. Have the Development team post the number of successful transactions to Amazon CloudWatch as a custom metric. Create a CloudWatch alarm when the threshold is breached, and use Amazon SNS to notify the Finance team.
C. Have the Development team log successful transactions to an application log. On each instance, set up the Amazon CloudWatch Logs agent to send application logs to CloudWatch Logs. Use an EC2 instance to monitor a metric filter,and send notifications to the Finance team.
D. Have the Development team log successful transactions to an application log. Set up the Amazon CloudWatch agent on each instance. Create a CloudWatch alarm when the threshold is breached, and use Amazon SNS to notify theFinance team.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 73**
A company is migrating an application to AWS that runs on a single Amazon EC2 instance. Because of licensing limitations, the application does not support horizontal scaling. The application will be using Amazon Aurora for its database.
How can the DevOps Engineer architect automated healing to automatically recover from EC2 and Aurora failures, in addition to recovering across Availability Zones (AZs), in the MOST cost-effective manner?

A. Create an EC2 Auto Scaling group with a minimum and maximum instance count of 1, and have it span across AZs. Use a single-node Aurora instance.
B. Create an EC2 instance and enable instance recovery. Create an Aurora database with a read replica in a second AZ, and promote it to a primary database instance if the primary database instance fails.
C. Create an Amazon CloudWatch Events rule to trigger an AWS Lambda function to start a new EC2 instance in an available AZ when the instance status reaches a failure state. Create an Aurora database with a read replica in a secondAZ, and promote it to a primary database instance when the primary database instance fails.
D. Assign an Elastic IP address on the instance. Create a second EC2 instance in a second AZ. Create an Amazon CloudWatch Events rule to trigger an AWS Lambda function to move the Elastic IP address to the second instance whenthe first instance fails. Use a single-node Aurora instance.



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

**Explanation/Reference:**

**QUESTION 74**
An Application team has three environments for their application: development, pre-production, and production. The team recently adopted AWS CodePipeline. However, the team has had several deployments of misconfigured or nonfunctional development code into the production environment, resulting in user disruption and downtime. The DevOps Engineer must review the pipeline and add steps to identify problems with the application before it is deployed.
What should the Engineer do to identify functional issues during the deployment process? (Choose two.)

A. Use Amazon Inspector to add a test action to the pipeline. Use the Amazon Inspector Runtime Behavior Analysis Inspector rules package to check that the deployed code complies with company security standards before deploying it toproduction.
B. Using AWS CodeBuild to add a test action to the pipeline to replicate common user activities and ensure that the results are as expected before progressing to production deployment.
C. Create an AWS CodeDeploy action in the pipeline with a deployment configuration that automatically deploys the application code to a limited number of instances. The action then pauses the deployment so that the QA team can reviewthe application functionality. When the review is complete, CodeDeploy resumes and deploys the application to the remaining production Amazon EC2 instances.

D. After the deployment process is complete, run a testing activity on an Amazon EC2 instance in a different region that accesses the application to simulate user behavior. If unexpected results occur, the testing activity sends a warning toan Amazon SNS topic. Subscribe to the topic to get updates.

E. Add an AWS CodeDeploy action in the pipeline to deploy the latest version of the development code to pre-production. Add a manual approval action in the pipeline so that the QA team can test and confirm the expected functionality.After the manual approval action, add a second CodeDeploy action that deploys the approved code to the production environment.

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

**Explanation/Reference:**

**QUESTION 75**
A DevOps Engineer is responsible for the deployment of a PHP application. The Engineer is working in a hybrid deployment, with the application running on both on-premises servers and Amazon EC2 instances. The application needs access to a database containing highly confidential information. Application instances need access to database credentials, which must be encrypted at rest and in transit before reaching the instances.
How should the Engineer automate the deployment process while also meeting the security requirements?

A. Use AWS Elastic Beanstalk with a PHP platform configuration to deploy application packages to the instances. Store database credentials on AWS Systems Manager Parameter Store using the Secure String data type. Define an IAMrole for Amazon EC2 allowing access, and decrypt only the database credentials. Associate this role to all the instances.

B. Use AWS CodeDeploy to deploy application packages to the instances. Store database credentials on AWS Systems Manager Parameter Store using the Secure String data type. Define an IAM policy for allowing access, and decryptonly the database credentials. Attach the IAM policy to the role associated to the instance profile for CodeDeploy-managed instances, and to the role used for on-premises instances registration on CodeDeploy.

C. Use AWS CodeDeploy to deploy application packages to the instances. Store database credentials on AWS Systems Manager Parameter Store using the Secure String data type. Define an IAM role with an attached policy that allowsdecryption of the database credentials. Associate this role to all the instances and on-premises servers.

D. Use AWS CodeDeploy to deploy application packages to the instances. Store database credentials in the AppSpec file. Define an IAM policy for allowing access to only the database credentials. Attach the IAM policy to the roleassociated to the instance profile for CodeDeploy-managed instances and the role used for on-premises instances registration on CodeDeploy.

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

**Explanation/Reference:**

**QUESTION 76**

A company has a single Developer writing code for an automated deployment pipeline. The Developer is storing source code in an Amazon S3 bucket for each project. The company wants to add more Developers to the team but is concerned about code conflicts and lost work. The company also wants to build a test environment to deploy newer versions of code for testing and allow Developers to automatically deploy to both environments when code is changed in the repository.
What is the MOST efficient way to meet these requirements?

A. Create an AWS CodeCommit repository for each project, use the master branch for production code, and create a testing branch for code deployed to testing. Use feature branches to develop new features and pull requests to mergecode to testing and master branches.
B. Create another S3 bucket for each project for testing code, and use an AWS Lambda function to promote code changes between testing and production buckets. Enable versioning on all buckets to prevent code conflicts.
C. Create an AWS CodeCommit repository for each project, and use the master branch for production and test code with different deployment pipelines for each environment. Use feature branches to develop new features.
D. Enable versioning and branching on each S3 bucket, use the master branch for production code, and create a testing branch for code deployed to testing. Have Developers use each branch for developing in each environment.

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

**Explanation/Reference:**



**QUESTION 77**
After presenting a working proof of concept for a new application that uses AWS API Gateway, a Developer must set up a team development environment for the project. Due to a tight timeline, the Developer wants to minimize time spent on infrastructure setup, and would like to reuse the code repository created for the proof of concept. Currently, all source code is stored in AWS CodeCommit.
Company policy mandates having alpha, beta, and production stages with separate Jenkins servers to build code and run tests for every stage. The Development Manager must have the ability to block code propagation between admins at any time. The Security team wants to make sure that users will not be able to modify the environment without permission. How can this be accomplished?

A. Create API Gateway alpha, beta, and production stages. Create a CodeCommit trigger to deploy code to the different stages using an AWS Lambda function.
B. Create API Gateway alpha, beta, and production stages. Create an AWS CodePipeline that pulls code from the CodeCommit repository. Create CodePipeline actions to deploy code to the API Gateway stages.
C. Create Jenkins servers for the alpha, beta, and production stages on Amazon EC2 instances. Create multiple CodeCommit triggers to deploy code to different stages using an AWS Lambda function.
D. Create an AWS CodePipeline pipeline that pulls code from the CodeCommit repository. Create alpha, beta, and production stages with Jenkins servers on CodePipeline.

**Correct Answer:** D

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

**Explanation/Reference:**

**QUESTION 78**
An online company uses Amazon EC2 Auto Scaling extensively to provide an excellent customer experience while minimizing the number of running EC2 instances. The company's self-hosted Puppet environment in the application layer manages the configuration of the instances. The IT manager wants the lowest licensing costs and wants to ensure that whenever the EC2 Auto Scaling group scales down, removed EC2 instances are deregistered from the Puppet master as soon as possible.
How can the requirement be met?

A. At instance launch time, use EC2 user data to deploy the AWS CodeDeploy agent. Use CodeDeploy to install the Puppet agent. When the Auto Scaling group scales out, run a script to register the newly deployed instances to the Puppetmaster. When the Auto Scaling group scales in, use the EC2 Auto Scaling EC2_INSTANCE_TERMINATING lifecycle hook to trigger de-registration from the Puppet master.
B. Bake the AWS CodeDeploy agent into the base AMI. When the Auto Scaling group scales out, use CodeDeploy to install the Puppet agent, and execute a script to register the newly deployed instances to the Puppet master. When theAuto Scaling group scales in, use the CodeDeploy ApplicationStop lifecycle hook to run a script to de-register the instance from the Puppet master.
C. At instance launch time, use EC2 user data to deploy the AWS CodeDeploy agent. When the Auto Scaling group scales out, use CodeDeploy to install the Puppet agent, and run a script to register the newly deployed instances to thePuppet master. When the Auto Scaling group scales in, use the EC2 user data instance stop script to run a script to de-register the instance from the Puppet master.
D. Bake the AWS Systems Manager agent into the base AMI. When the Auto Scaling group scales out, use the AWS Systems Manager to install the Puppet agent, and run a script to register the newly deployed instances to the Puppetmaster. When the Auto Scaling group scales in, use the Systems Manager instance stop lifecycle hook to run a script to de-register the instance from the Puppet master.

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

**Explanation/Reference:**

**QUESTION 79**
A company discovers that some IAM users have been storing their AWS access keys in configuration files that have been pushed to a Git repository hosting service. Which solution will require the LEAST amount of management overhead while preventing the exposed AWS access keys from being used?

A. Build an application that will create a list of all AWS access keys in the account and search each key on Git repository hosting services. If a match is found, configure the application to disable the associated access key. Then deploy theapplication to an AWS Elastic Beanstalk worker environment and define a periodic task to invoke the application every hour.

B. Use Amazon Inspector to detect when a key has been exposed online. Have Amazon Inspector send a notification to an Amazon SNS topic when a key has been exposed. Create an AWS Lambda function subscribed to the SNS topic todisable the IAM user to whom the key belongs, and then delete the key so that it cannot be used.

C. Configure AWS Trusted Advisor and create an Amazon CloudWatch Events rule that uses Trusted Advisor as the event source. Configure the CloudWatch Events rule to invoke an AWS Lambda function as the target. If the Lambdafunction finds the exposed access keys, then have it disable the access key so that it cannot be used.

D. Create an AWS Config rule to detect when a key is exposed online. Haw AWS Config send change notifications to an SNS topic. Configure an AWS Lambda function that is subscribed to the SNS topic to check the notification sent byAWS Config, and then disable the access key so it cannot be used.

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

**Explanation/Reference:**

**QUESTION 80**
Company policies require that information about IP traffic going between instances in the production Amazon VPC is captured. The capturing mechanism must always be enabled and the Security team must be notified when any changes in configuration occur.
What should be done to ensure that these requirements are met?



A. Using the UserData section of an AWS CloudFormation template, install tcpdump on every provisioned Amazon EC2 instance. The output of the tool is sent to Amazon EFS for aggregation and querying. In addition, scheduling an Amazon CloudWatch Events rule calls an AWS Lambda function to check whether tcpdump is up and running and sends an email to the security organization when there is an exception.

B. Create a flow log for the production VPC and assign an Amazon S3 bucket as a destination for delivery. Using Amazon S3 Event Notification, set up an AWS Lambda function that is triggered when a new log file gets delivered. ThisLambda function updates an entry in Amazon DynamoDB, which is periodically checked by scheduling an Amazon CloudWatch Events rule to notify security when logs have not arrived.

C. Create a flow log for the production VPC. Create a new rule using AWS Config that is triggered by configuration changes of resources of type 'EC2:VPC'. As part of configuring the rule, create an AWS Lambda function that looks up flowlogs for a given VPC. If the VPC flow logs are not configured, return a 'NON_COMPLIANT' status and notify the security organization.

D. Configure a new trail using AWS CloudTrail service. Using the UserData section of an AWS CloudFormation template, install tcpdump on every provisioned Amazon EC2 instance. Connect Amazon Athena to the CloudTrail and write an AWS Lambda function that monitors for a flow log disable event. Once the CloudTrail entry has been spotted, alert the security organization.

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

**Explanation/Reference:**

**QUESTION 81**
A DevOps Engineer needs to deploy a scalable three-tier Node.js application in AWS. The application must have zero downtime during deployments and be able to roll back to previous versions. Other applications will also connect to the same MySQL backend database.
The CIO has provided the following guidance for logging:
- Centrally view all current web access server logs.
- Search and filter web and application logs in near-real time.
- Retain log data for three months.

How should these requirements be met?

A. Deploy the application using AWS Elastic Beanstalk. Configure the environment type for Elastic Load Balancing and Auto Scaling. Create an Amazon RDS MySQL instance inside the Elastic Beanstalk stack. Configure the ElasticBeanstalk log options to stream logs to Amazon CloudWatch Logs. Set retention to 90 days.
B. Deploy the application on Amazon EC2. Configure Elastic Load Balancing and Auto Scaling. Use an Amazon RDS MySQL instance for the database tier. Configure the application to store log files in Amazon S3. Use Amazon EMR tosearch and filter the data. Set an Amazon S3 lifecycle rule to expire objects after 90 days.
C. Deploy the application using AWS Elastic Beanstalk. Configure the environment type for Elastic Load Balancing and Auto Scaling. Create the Amazon RDS MySQL instance outside the Elastic Beanstalk stack. Configure the ElasticBeanstalk log options to stream logs to Amazon CloudWatch Logs. Set retention to 90 days.
D. Deploy the application on Amazon EC2. Configure Elastic Load Balancing and Auto Scaling. Use an Amazon RDS MySQL instance for the database tier. Configure the application to load streaming log data using Amazon Kinesis DataFirehose into Amazon ES. Delete and create a new Amazon ES domain every 90 days.

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

**Explanation/Reference:**
Explanation:
The Amazon EC2 instances in your Elastic Beanstalk environment generate logs that you can view to troubleshoot issues with your application or configuration files. Logs created by the web server, application server, Elastic Beanstalk platform scripts, and AWS CloudFormation are stored locally on individual instances. You can easily retrieve them by using the environment management console or the EB CLI. You can also configure your environment to stream logs to Amazon CloudWatch Logs in real-time.

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

**QUESTION 82**
An IT team has built an AWS CloudFormation template so others in the company can quickly and reliably deploy and terminate an application. The template

creates an Amazon EC2 instance with a user data script to install the application and an Amazon S3 bucket that the application uses to serve static webpages while it is running.
All resources should be removed when the CloudFormation stack is deleted. However, the team observes that CloudFormation reports an error during stack deletion, and the S3 bucket created by the stack is not deleted. How can the team resolve the error in the MOST efficient manner to ensure that all resources are deleted without errors?

A. Add DeletionPolicy attribute to the S3 bucket resource, with the value Delete forcing the bucket to be removed when the stack is deleted.
B. Add a custom resource when an AWS Lambda function with the DependsOn attribute specifying the S3 bucket, and an IAM role. Writhe the Lambda function to delete all objects from the bucket when the RequestType is Delete.
C. Identify the resource that was not deleted. From the S3 console, empty the S3 bucket and then delete it.
D. Replace the EC2 and S3 bucket resources with a single AWS OpsWorks Stacks resource. Define a custom recipe for the stack to create and delete the EC2 instance and the S3 bucket.

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

**Explanation/Reference:**



**QUESTION 83**
A DevOps Engineer just joined a new company that is already running workloads on Amazon EC2 instances. AWS has been adopted incrementally with no central governance. The Engineer must now assess how well the existing deployments comply with the following requirements:
EC2 instances are running only approved AMIs.
Amazon EBS volumes are encrypted.
EC2 instances have an Owner tag.
Root login over SSH is disabled on EC2 instances.
Which services should the Engineer use to perform this assessment with the LEAST amount of effort? (Select TWO.)

A. AWS Config
B. Amazon GuardDuty
C. AWS System Manager
D. AWS Directory Service
E. Amazon Inspector

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

**Explanation/Reference:**

**QUESTION 84**
A healthcare company has a critical application running in AWS. Recently, the company experienced some down time. if it happens again, the company needs to be able to recover its application in another AWS Region. The application uses Elastic Load Balancing and Amazon EC2 instances. The company also maintains a custom AMI that contains its application. This AMI is changed frequently.
The workload is required to run in the primary region, unless there is a regional service disruption, in which case traffic should fail over to the new region. Additionally, the cost for the second region needs to be low. The RTO is 2 hours. Which solution allows the company to fail over to another region in the event of a failure, and also meet the above requirements?

A. Maintain a copy of the AMI from the main region in the backup region. Create an Auto Scaling group with one instance using a launch configuration that contains the copied AMI. Use an Amazon Route 53 record to direct traffic to the loadbalancer in the backup region in the event of failure, as required. Allow the Auto Scaling group to scale out as needed during a failure.
B. Automate the copying of the AMI in the main region to the backup region. Generate an AWS Lambda function that will create an EC2 instance from the AMI and place it behind a load balancer. Using the same Lambda function, point theAmazon Route 53 record to the load balancer in the backup region. Trigger the Lambda function in the event of a failure.
C. Place the AMI in a replicated Amazon S3 bucket. Generate an AWS Lambda function that can create a launch configuration and assign it to an already created Auto Scaling group. Have one instance in this Auto Scaling group ready toaccept traffic. Trigger the Lambda function in the event of a failure. Use an Amazon Route 53 record and modify it with the same Lambda function to point to the load balancer in the backup region.
D. Automate the copying of the AMI to the backup region. Create an AWS Lambda function that can create a launch configuration and assign it to an already created Auto Scaling group. Set the Auto Scaling group maximum size to 0 andonly increase it with the Lambda function during a failure. Trigger the Lambda function in the event of a failure. Use an Amazon Route 53 record and modify it with the same Lambda function to point to the load balancer in the backup region.

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

**Explanation/Reference:**

**QUESTION 85**
A legacy web application stores access logs in a proprietary text format. One of the security requirements is to search application access events and correlate them with access data from many different systems. These searches should be near-real time.
Which solution offloads the processing load on the application server and provides a mechanism to search the data in near-real time?

A. Install the Amazon CloudWatch Logs agent on the application server and use CloudWatch Events rules to search logs for access events. Use Amazon CloudSearch as an interface to search for events.
B. Use the third-party file-input plugin Logstash to monitor the application log file, then use a custom dissect filter on the agent to parse the log entries into the

JSON format. Output the events to Amazon ES to be searched. Use theElasticsearch API for querying the data.

C. Upload the log files to Amazon S3 by using the S3 sync command. Use Amazon Athena to define the structure of the data as a table, with Athena SQL queries to search for access events.

D. Install the Amazon Kinesis Agent on the application server, configure it to monitor the log files, and send it to a Kinesis stream. Configure Kinesis to transform the data by using an AWS Lambda function, and forward events to AmazonES for analysis. Use the Elasticsearch API for querying the data.

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

**Explanation/Reference:**

**QUESTION 86**
A company runs a database on a single Amazon EC2 instance in a development environment. The data is stored on separate Amazon EBS volumes that are attached to the EC2 instance. An Amazon Route 53 A record has been created and configured to point to the EC2 instance. The company would like to automate the recovery of the database instance when an instance or Availability Zone (AZ) fails. The company also wants to keep its costs low. The RTO is 4 hours and RPO is 12 hours.
Which solution should a DevOps Engineer implement to meet these requirements?

A. Run the database in an Auto Scaling group with a minimum and maximum instance count of 1 in multiple AZs. Add a lifecycle hook to the Auto Scaling group and define an Amazon CloudWatch Events rule that is triggered when alifecycle event occurs. Have the CloudWatch Events rule invoke an AWS Lambda function to detach or attach the Amazon EBS data volumes from the EC2 instance based on the event. Configure the EC2 instance UserData to mount the data volumes (retry on failure with a short delay), then start the database and update the Route 53 record.

B. Run the database on two separate EC2 instances in different AZs with one active and the other as a standby. Attach the data volumes to the active instance. Configure an Amazon CloudWatch Events rule to invoke an AWS Lambdafunction on EC2 instance termination. The Lambda function launches a replacement EC2 instance. If the terminated instance was the active node, then the function attaches the data volumes to the standby node. Start the database and update the Route 53 record.

C. Run the database in an Auto Scaling group with a minimum and maximum instance count of 1 in multiple AZs. Create an AWS Lambda function that is triggered by a scheduled Amazon CloudWatch Events rule every 4 hours to take asnapshot of the data volume and apply a tag. Have the instance UserData get the latest snapshot, create a new volume from it, and attach and mount the volume. Then start the database and update the Route 53 record.

D. Run the database on two separate EC2 instances in different AZs. Configure one of the instances as a master and the other as a standby. Set up replication between the master and standby instances. Point the Route 53 record to themaster. Configure an Amazon CloudWatch Events rule to invoke an AWS Lambda function upon the EC2 instance termination. The Lambda function launches a replacement EC2 instance. If the terminated instance was the active node, the function promotes the standby to master and points the Route 53 record to it.

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

**Explanation/Reference:**

**QUESTION 87**
A consulting company was hired to assess security vulnerabilities within a client company's application and propose a plan to remediate all identified issues. The architecture is identified as follows: Amazon S3 storage for content, an Auto Scaling group of Amazon EC2 instances behind an Elastic Load Balancer with attached Amazon EBS storage, and an Amazon RDS MySQL database. There are also several AWS Lambda functions that communicate directly with the RDS database using connection string statements in the code.
The consultants identified the top security threat as follows: the application is not meeting its requirement to have encryption at rest.
What solution will address this issue with the LEAST operational overhead and will provide monitoring for potential future violations?

A. Enable SSE encryption on the S3 buckets and RDS database. Enable OS-based encryption of data on EBS volumes. Configure Amazon Inspector agents on EC2 instances to report on insecure encryption ciphers. Set up AWS Configrules to periodically check for non-encrypted S3 objects.
B. Configure the application to encrypt each file prior to storing on Amazon S3. Enable OS-based encryption of data on EBS volumes. Encrypt data on write to RDS. Run cron jobs on each instance to check for unencrypted data and notify viaAmazon SNS. Use S3 Events to call an AWS Lambda function and verify if the file is encrypted.
C. Enable Secure Sockets Layer (SSL) on the load balancer, ensure that AWS Lambda is using SSL to communicate to the RDS database, and enable S3 encryption. Configure the application to force SSL for incoming connections andconfigure RDS to only grant access if the session is encrypted. Configure Amazon Inspector agents on EC2 instances to report on insecure encryption ciphers.
D. Enable SSE encryption on the S3 buckets, EBS volumes, and the RDS database. Store RDS credentials in EC2 Parameter Store. Enable a policy on the S3 bucket to deny unencrypted puts. Set up AWS Config rules to periodicallycheck for non-encrypted S3 objects and EBS volumes, and to ensure that RDS storage is encrypted.

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

**Explanation/Reference:**

**QUESTION 88**
A new zero-day vulnerability was found in OpenSSL requiring the immediate patching of a production web fleet running on Amazon Linux. Currently, OS updates are performed manually on a monthly basis and deployed using updates to the production Auto Scaling Group's launch configuration.
Which method should a DevOps Engineer use to update packages in-place without downtime?

A. Use AWS CodePipline and AWS CodeBuild to generate new copies of these packages, and update the Auto Scaling group's launch configuration.
B. Use AWS Inspector to run "yum upgrade" on all running production instances, and manually update the AMI for the next maintenance window.
C. Use Amazon EC2 Run Command to issue a package update command to all running production instances, and update the AMI for future deployments.
D. Define a new AWS OpsWorks layer to match the running production instances, and use a recipe to issue a package update command to all running production instances.

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

**Explanation/Reference:**

**QUESTION 89**
A company runs a production application workload in a single AWS account that uses Amazon Route 53, AWS Elastic Beanstalk, and Amazon RDS. In the event of a security incident, the Security team wants the application workload to fail over to a new AWS account. The Security team also wants to block all access to the original account immediately, with no access to any AWS resources in the original AWS account, during forensic analysis. What is the most cost-effective way to prepare to fail over to the second account prior to a security incident?

A. Migrate the Amazon Route 53 configuration to a dedicated AWS account. Mirror the Elastic Beanstalk configuration in a different account. Enable RDS Database Read Replicas in a different account.
B. Migrate the Amazon Route 53 configuration to a dedicated AWS account. Save/copy the Elastic Beanstalk configuration files in a different AWS account. Copy snapshots of the RDS Database to a different account.
C. Save/copy the Amazon Route 53 configurations for use in a different AWS account after an incident. Save/copy Elastic Beanstalk configuration files to a different account. Enable the RDS database read replica in a different account.
D. Save/copy the Amazon Route 53 configurations for use in a different AWS account after an incident. Mirror the configuration of Elastic Beanstalk in a different account. Copy snapshots of the RDS database to a different account.

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

**Explanation/Reference:**

**QUESTION 90**
Two teams are working together on different portions of an architecture and are using AWS CloudFormation to manage their resources. One team administers operating system-level updates and patches, while the other team manages application-level dependencies and updates. The Application team must take the most recent AMI when creating new instances and deploying the application. What is the MOST scalable method for linking these two teams and processes?

A. The Operating System team uses CloudFormation to create new versions of their AMIs and lists the Amazon Resource names (ARNs) of the AMIs in an encrypted Amazon S3 object as part of the stack output section. The Applicationteam uses a cross-stack reference to load the encrypted S3 object and obtain the most recent AMI ARNs.
B. The Operating System team uses CloudFormation stack to create an AWS CodePipeline pipeline that builds new AMIs, then places the latest AMI ARNs in an encrypted Amazon S3 object as part of the pipeline output. The Applicationteam uses a cross-stack reference within their own CloudFormation template to get

that S3 object location and obtain the most recent AMI ARNs to use when deploying their application.

C. The Operating System team uses CloudFormation stack to create an AWS CodePipeline pipeline that builds new AMIs. The team then places the AMI ARNs as parameters in AWS Systems Manager Parameter Store as part of thepipeline output. The Application team specifies a parameter of type ssm in their CloudFormation stack to obtain the most recent AMI ARN from the Parameter Store.

D. The Operating System team maintains a nested stack that includes both the operating system and Application team templates. The Operating System team uses a stack update to deploy updates to the application stack whenever theApplication team changes the application code.

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

**Explanation/Reference:**

**QUESTION 91**
The Development team has grown substantially in recent months and so has the number of projects that use separate code repositories. The current process involves configuring AWS CodePipeline manually. There have been service limit alerts regarding the number of Amazon S3 buckets that exist.

Which pipeline option will reduce S3 bucket sprawl alerts?

A. Combine the multiple separate code repositories into a single one, and deploy using an AWS CodePipeline that has logic for each project.

B. Create new pipelines by using the AWS API or AWS CLI, and configure them to use a single S3 bucket with separate prefixes for each project.

C. Create a new pipeline in a different region for each project to bypass the service limits for S3 buckets in a single region.

D. Create a new pipeline and S3 bucket for each project by using the AWS API or AWS CLI to bypass the service limits for S3 buckets in a single account.

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

**Explanation/Reference:**

**QUESTION 92**
A startup company is developing a web application on AWS. It plans to use Amazon RDS for persistence and deploy the application to Amazon EC2 with an Auto Scaling group. The company would also like to separate the environments for development, testing, and production.

What is the MOST secure approach to manage the application configuration?

A. Create a property file to include the configuration and the encrypted passwords. Check in the property file to the source repository, package the property file

with the application, and deploy the application. Create an environment tag forthe EC2 instances and tag the instances respectively. The application will extract the necessary property values based on the environment tag.

B. Create a property file for each environment to include the environment-specific configuration and an encrypted password. Check in the property files to the source repository. During deployment, use only the environment-specific propertyfile with the application. The application will read the needed property values from the deployed property file.

C. Create a property file for each environment to include the environment-specific configuration. Create a private Amazon S3 bucket and save the property files in the bucket. Save the passwords in the bucket with AWS KMS encryption.During deployment, the application will read the needed property values from the environment-specific property file in the S3 bucket.

D. Create a property file for each environment to include the environment-specific configuration. Create a private Amazon S3 bucket and save the property files in the bucket. Save the encrypted passwords in the AWS Systems ManagerParameter Store. Create an environment tag for the EC2 instances and tag the instances respectively. The application will read the needed property values from the environment-specific property file in the S3 bucket and the parameter store.

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

**Explanation/Reference:**



**QUESTION 93**
A DevOps Engineer is using AWS CodeDeploy across a fleet of Amazon EC2 instances in an EC2 Auto Scaling group. The associated CodeDeploy deployment group, which is integrated with EC2 Auto Scaling, is configured to perform inplace deployments with CodeDeployDefault.OneAtATime. During an ongoing new deployment, the Engineer discovers that, although the overall deployment finished successfully, two out of five instances have the previous application revision deployed. The other three instances have the newest application revision. What is likely causing this issue?

A. The two affected instances failed to fetch the new deployment.

B. A failed AfterInstall lifecycle event hook caused the CodeDeploy agent to roll back to the previous version on the affected instances.

C. The CodeDeploy agent was not installed in two affected instances.

D. EC2 Auto Scaling launched two new instances while the new deployment had not yet finished, causing the previous version to be deployed on the affected instances.

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

**Explanation/Reference:**

**QUESTION 94**
A company runs a three-tier web application in its production environment, which is built on a single AWS CloudFormation template made up of Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. Data is stored in an Amazon RDS Multi-AZ DB instance with read replicas. Amazon Route 53 manages the application's public DNS record.
A DevOps Engineer must create a workflow to mitigate a failed software deployment by rolling back changes in the production environment when a software cutover occurs for new application software. What steps should the Engineer perform to meet these requirements with the LEAST amount of downtime?

A. Use CloudFormation to deploy an additional staging environment and configure the Route 53 DNS with weighted records. During cutover, change the Route 53 A record weights to achieve an even traffic distribution between the twoenvironments. Validate the traffic in the new environment and immediately terminate the old environment if tests are successful.
B. Use a single AWS Elastic Beanstalk environment to deploy the staging and production environments. Update the environment by uploading the ZIP file with the new application code. Swap the Elastic Beanstalk environment CNAME.Validate the traffic in the new environment and immediately terminate the old environment if tests are successful.
C. Use a single AWS Elastic Beanstalk environment and an AWS OpsWorks environment to deploy the staging and production environments. Update the environment by uploading the ZIP file with the new application code into the ElasticBeanstalk environment deployed with the OpsWorks stack. Validate the traffic in the new environment and immediately terminate the old environment if tests are successful.
D. Use AWS CloudFormation to deploy an additional staging environment, and configure the Route 53 DNS with weighted records. During cutover, increase the weight distribution to have more traffic directed to the new staging environmentas workloads are successfully validated. Keep the old production environment in place until the new staging environment handles all traffic.



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

**Explanation/Reference:**

**QUESTION 95**
A company wants to adopt a methodology for handling security threats from leaked and compromised IAM access keys. The DevOps Engineer has been asked to automate the process of acting upon compromised access keys, which includes identifying users, revoking their permissions, and sending a notification to the Security team.
Which of the following would achieve this goal?

A. Use the AWS Trusted Advisor generated security report for access keys. Use Amazon EMR to run analytics on the report. Identify compromised IAM access keys and delete them. Use Amazon CloudWatch with an EMR Cluster StateChange event to notify the Security team.
B. Use AWS Trusted Advisor to identify compromised access keys. Create an Amazon CloudWatch Events rule with Trusted Advisor as the event source, and AWS Lambda and Amazon SNS as targets. Use AWS Lambda to deletecompromised IAM access keys and Amazon SNS to notify the Security team.
C. Use the AWS Trusted Advisor generated security report for access keys. Use AWS Lambda to scan through the report. Use scan result inside AWS Lambda and delete compromised IAM access keys. Use Amazon SNS to notify theSecurity team.
D. Use AWS Lambda with a third-party library to scan for compromised access keys. Use scan result inside AWS Lambda and delete compromised IAM access

keys. Create Amazon CloudWatch custom metrics for compromised keys.Create a CloudWatch alarm on the metrics to notify the Security team.

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

**Explanation/Reference:**
Reference https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

**QUESTION 96**
A company wants to use Amazon ECS to provide a Docker container runtime environment. For compliance reasons, all Amazon EBS volumes used in the ECS cluster must be encrypted. Rolling updates will be made to the cluster instances and the company wants the instances drained of all tasks before being terminated.
How can these requirements be met? (Select TWO.)

A. Modify the default ECS AMI user data to create a script that executes docker rm -f {id} for all running container instances. Copy the script to the /etc/init.d/rc.d directory and execute chconfig enabling the script to run during operating system shutdown.
B. Use AWS CodePipeline to build a pipeline that discovers the latest Amazon-provided ECS AMI, then copies the image to an encrypted AMI outputting the encrypted AMI ID. Use the encrypted AMI ID when deploying the cluster.
C. Copy the default AWS CloudFormation template that ECS uses to deploy cluster instances. Modify the template resource EBS configuration setting to set 'Encrypted: True' and include the AWS KMS alias: 'aws/ebs' to encrypt the AMI.
D. Create an Auto Scaling lifecycle hook backed by an AWS Lambda function that uses the AWS SDK to mark a terminating instance as DRAINING. Prevent the lifecycle hook from completing until the running tasks on the instance are zero.
E. Create an IAM role that allows the action ECS::EncryptedImage. Configure the AWS CLI and a profile to use this role. Start the cluster using the AWS CLI providing the --use-encrypted-image and --kms-key arguments to the create-cluster ECS command.

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

**Explanation/Reference:**

**QUESTION 97**
A government agency has multiple AWS accounts, many of which store sensitive citizen information. A Security team wants to detect anomalous account and network activities (such as SSH brute force attacks) in any account and centralize that information in a dedicated security account. Event information should be stored in an Amazon S3 bucket in the security account, which is monitored by the department's Security Information and Even Manager (SIEM) system. How can this be accomplished?

A. Enable Amazon Macie in every account. Configure the security account as the Macie Administrator for every member account using invitation/acceptance.

Create an Amazon CloudWatch Events rule in the security account to send allfindings to Amazon Kinesis Data Firehose, which should push the findings to the S3 bucket.

B. Enable Amazon Macie in the security account only. Configure the security account as the Macie Administrator for every member account using invitation/ acceptance. Create an Amazon CloudWatch Events rule in the security account to send all findings to Amazon Kinesis Data Streams. Write an application using KCL to read data from the Kinesis Data Streams and write to the S3 bucket.

C. Enable Amazon GuardDuty in every account. Configure the security account as the GuardDuty Administrator for every member account using invitation/ acceptance. Create an Amazon CloudWatch rule in the security account to send all findings to Amazon Kinesis Data Firehose, which will push the findings to the S3 bucket.

D. Enable Amazon GuardDuty in the security account only. Configure the security account as the GuardDuty Administrator for every member account using invitation/acceptance. Create an Amazon CloudWatch rule in the security accountto send all findings to Amazon Kinesis Data Streams. Write an application using KCL to read data from Kinesis Data Streams and write to the S3 bucket.

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

**Explanation/Reference:**

**QUESTION 98**
An AWS CodePipeline pipeline has implemented a code release process. The pipeline is integrated with AWS CodeDeploy to deploy versions of an application to multiple Amazon EC2 instances for each CodePipeline stage. During a recent deployment, the pipeline failed due to a CodeDeploy issue. The DevOps team wants to improve monitoring and notifications during deployment to decrease resolution times. What should the DevOps Engineer do to create notifications when issues are discovered?

A. Implement AWS CloudWatch Logs for CodePipeline and CodeDeploy, create an AWS Config rule to evaluate code deployment issues, and create an Amazon SNS topic to notify stakeholders of deployment issues.

B. Implement AWS CloudWatch Events for CodePipeline and CodeDeploy, create an AWS Lambda function to evaluate code deployment issues, and create an Amazon SNS topic to notify stakeholders of deployment issues.

C. Implement AWS CloudTrail to record CodePipeline and CodeDeploy API call information, create an AWS Lambda function to evaluate code deployment issues, and create an Amazon SNS topic to notify stakeholders of deploymentissues.

D. Implement AWS CloudWatch Events for CodePipeline and CodeDeploy, create an Amazon Inspector assessment target to evaluate code deployment issues, and create an Amazon SNS topic to notify stakeholders of deployment issues.

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

**Explanation/Reference:**

**QUESTION 99**
A company runs an application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones in us-east1. The application stores data in an Amazon RDS MySQL Multi-AZ DB instance.
A DevOps Engineer wants to modify the current solution and create a hot standby of the environment in another region to minimize downtime if a problem occurs in us-east-1.
Which combination of steps should the DevOps Engineer take to meet these requirements? (Select THREE.)

A. Add a health check to the Amazon Route 53 alias record to evaluate the health of the primary region. Use AWS Lambda, configured with an Amazon CloudWatch Events trigger, to promote the Amazon RDS read replica in the disaster recoveryregion.
B. Create a new Application Load Balancer and Amazon EC2 Auto Scaling group in the disaster recovery region.
C. Extend the current Amazon EC2 Auto Scaling group to the subnets in the disaster recovery region.
D. Enable multi-region failover for the RDS configuration for the database instance.
E. Deploy a read replica of the RDS instance in the disaster recovery region.
F. Create an AWS Lambda function to evaluate the health of the primary region. If it fails, modify the Amazon Route 53 record to point at the disaster recovery region and promote the RDS read replica

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



**Explanation/Reference:**

**QUESTION 100**
A DevOps Engineer needs to design and implement a backup mechanism for Amazon EFS. The Engineer is given the following requirements:
- The backup should run on schedule.
- The backup should be stopped if the backup window expires.
- The backup should be stopped if the backup completes before the backup window.
- The backup logs should be retained for further analysis.
- The design should support highly available and fault-tolerant paradigms.
- Administrators should be notified with backup metadata.

Which design will meet these requirements?

A. Use AWS Lambda with an Amazon CloudWatch Events rule for scheduling the start/stop of backup activity. Run backup scripts on Amazon EC2 in an Auto Scaling group. Use Auto Scaling lifecycle hooks and the SSM Run Command onEC2 for uploading backup logs to Amazon S3. Use Amazon SNS to notify administrators with backup activity metadata.
B. Use Amazon SWF with an Amazon CloudWatch Events rule for scheduling the start/stop of backup activity. Run backup scripts on Amazon EC2 in an Auto

Scaling group. Use Auto Scaling lifecycle hooks and the SSM Run Command onEC2 for uploading backup logs to Amazon Redshift. Use CloudWatch Alarms to notify administrators with backup activity metadata.

C. Use AWS Data Pipeline with an Amazon CloudWatch Events rule for scheduling the start/stop of backup activity. Run backup scripts on Amazon EC2 in a single Availability Zone. Use Auto Scaling lifecycle hooks and the SSM RunCommand on EC2 for uploading the backup logs to Amazon RDS. Use Amazon SNS to notify administrators with backup activity metadata.

D. Use AWS CodePipeline with an Amazon CloudWatch Events rule for scheduling the start/stop of backup activity. Run backup scripts on Amazon EC2 in a single Availability Zone. Use Auto Scaling lifecycle hooks and the SSM RunCommand on Amazon EC2 for uploading backup logs to Amazon S3. Use Amazon SES to notify admins with backup activity metadata.

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

**Explanation/Reference:**

**QUESTION 101**
A rapidly growing company wants to scale for Developer demand for AWS development environments. Development environments are created manually in the AWS Management Console. The Networking team uses AWS CloudFormation to manage the networking infrastructure, exporting stack output values for the Amazon VPC and all subnets. The development environments have common standards, such as Application Load Balancers, Amazon EC2 Auto Scaling groups, security groups, and Amazon DynamoDB tables.
To keep up with the demand, the DevOps Engineer wants to automate the creation of development environments. Because the infrastructure required to support the application is expected to grow, there must be a way to easily update the deployed infrastructure. CloudFormation will be used to create a template for the development environments. Which approach will meet these requirements and quickly provide consistent AWS environments for Developers?

A. Use Fn:ImportValue intrinsic functions in the Resources section of the template to retrieve Virtual Private Cloud (VPC) and subnet values. Use CloudFormation StackSets for the development environments, using the Count input parameter to indicate the number of environments needed. use the UpdateStackSet command to update existing development environments.

B. Use nested stacks to define common infrastructure components. To access the exported values, use TemplateURL to reference the Networking team's template. To retrieve Virtual Private Cloud (VPC) and subnet values, use Fn::ImportValue intrinsic functions in the Parameters section of the master template. Use the CreateChangeSet and ExecuteChangeSet commands to update existing development environments.

C. Use nested stacks to define common infrastructure components. Use Fn::ImportValue intrinsic functions with the resources of the nested stack to retrieve Virtual Private Cloud (VPC) and subnet values. Use the CreateChangeSet and ExecuteChangeSet commands to update existing development environments.

D. Use Fn:ImportValue intrinsic functions in the Parameters section of the master template to retrieve Virtual Private Cloud (VPC) and subnet values. Define the development resources in the order they need to be created in the CloudFormation nested stacks. Use the CreateChangeSet and ExecuteChangeSet commands to update existing development environments.

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

**Explanation/Reference:**

**QUESTION 102**
A company has a website in an AWS Elastic Beanstalk load balancing and automatic scaling environment. This environment has an Amazon RDS MySQL instance configured as its database resource. After a sudden increase in traffic, the website started dropping traffic. An administrator discovered that the application on some instances is not responding as the result of out-of-memory errors. Classic Load Balancer marked those instances as out of service, and the health status of Elastic Beanstalk enhanced health reporting is degraded. However, Elastic Beanstalk did not replace those instances. Because of the diminished capacity behind the Classic Load Balancer, the application response times are slower for the customers.
Which action will permanently fix this issue?

A. Clone the Elastic Beanstalk environment. When the new environment is up, swap CNAME and terminate the earlier environment.
B. Temporarily change the maximum number of instances in the Auto Scaling group to allow the group to support more traffic.
C. Change the setting for the Auto Scaling group health check from Amazon EC2 to Elastic Load Balancing, and increase the capacity of the group.
D. Write a cron script for restarting the web server process when memory is full, and deploy it with AWS Systems Manager.

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



**Explanation/Reference:**

**QUESTION 103**
A DevOps Engineer is launching a new application that will be deployed on infrastructure using Amazon Route 53, an Application Load Balancer, Auto Scaling, and Amazon DynamoDB. One of the key requirements of this launch is that the application must be able to scale to meet a load increase. During periods of low usage, the infrastructure components must scale down to optimize cost. What steps can the DevOps Engineer take to meet the requirements? (Select TWO.)

A. Use AWS Trusted Advisor to submit limit increase requests for the Amazon EC2 instances that will be used by the infrastructure.
B. Determine which Amazon EC2 instance limits need to be raised by leveraging AWS Trusted Advisor, and submit a request to AWS Support to increase those limits.
C. Enable Auto Scaling for the DynamoDB tables that are used by the application.
D. Configure the Application Load Balancer to automatically adjust the target group based on the current load.
E. Create an Amazon CloudWatch Events scheduled rule that runs every 5 minutes to track the current use of the Auto Scaling group. If usage has changed, trigger a scale-up event to adjust the capacity. Do the same for DynamoDB readand write capacities.

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

**Explanation**

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

**QUESTION 104**
A company hosts parts of a Python-based application using AWS Elastic Beanstalk. An Elastic Beanstalk CLI is being used to create and update the environments. The Operations team detected an increase in requests in one of the Elastic Beanstalk environments that caused downtime overnight. The team noted that the policy used for AWS Auto Scaling is NetworkOut. Based on load testing metrics, the team determined that the application needs to scale CPU utilization to improve the resilience of the environments. The team wants to implement this across all environments automatically. Following AWS recommendations, how should this automation be implemented?

A. Using ebextensions, place a command within the container_commands key to perform an API call to modify the scaling metric to CPUUtilization for the Auto Scaling configuration. Use leader_only to execute this command in only the first instance launched within the environment.
B. Using ebextensions, create a custom resource that modifies the AWSEBAutoScalingScaleUpPolicy and AWSEBAutoScalingScaleDownPolicy resources to use CPUUtilization as a metric to scale for the Auto Scaling group.
C. Using ebextensions, configure the option setting MeasureName to CPUUtilization within the aws:autoscaling:trigger namespace.
D. Using ebextensions, place a script within the files key and place it in /opt/elasticbeanstalk/hooks/appdeploy/pre to perform an API call to modify the scaling metric to CPUUtilization for the Auto Scaling configuration. Use leader_only to place this script in only the first instance launched within the environment.



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

**Explanation/Reference:**

**QUESTION 105**
A DevOps team needs to query information in application logs that are generated by an application running multiple Amazon EC2 instances deployed with AWS Elastic Beanstalk. Instance log streaming to Amazon CloudWatch Logs was enabled on Elastic Beanstalk. Which approach would be the MOST cost-efficient?

A. Use a CloudWatch Logs subscription to trigger an AWS Lambda function to send the log data to an Amazon Kinesis Data Firehose stream that has an Amazon S3 bucket destination. Use Amazon Athena to query the log data from thebucket.
B. Use a CloudWatch Logs subscription to trigger an AWS Lambda function to send the log data to an Amazon Kinesis Data Firehose stream that has an Amazon S3 bucket destination. Use a new Amazon Redshift cluster and AmazonRedshift Spectrum to query the log data from the bucket.
C. Use a CloudWatch Logs subscription to send the log data to an Amazon Kinesis Data Firehose stream that has an Amazon S3 bucket destination. Use Amazon Athena to query the log data from the bucket.
D. Use a CloudWatch Logs subscription to send the log data to an Amazon Kinesis Data Firehose stream that has an Amazon S3 bucket destination. Use a new Amazon Redshift cluster and Amazon Redshift Spectrum to query the logdata from the bucket.

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

**Explanation/Reference:**

**QUESTION 106**
A company's web application will be migrated to AWS. The application is designed so that there is no server-side code required. As part of the migration, the company would like to improve the security of the application by adding HTTP response headers, following the Open Web Application Security Project (OWASP) secure headers recommendations. How can this solution be implemented to meet the security requirements using best practices?

A. Use an Amazon S3 bucket configured for website hosting, then set up server access logging on the S3 bucket to track user activity. Then configure the static website hosting and execute a scheduled AWS Lambda function to verify, andif missing, add security headers to the metadata.
B. Use an Amazon S3 bucket configured for website hosting, then set up server access logging on the S3 bucket to track user activity. Configure the static website hosting to return the required security headers.
C. Use an Amazon S3 bucket configured for website hosting. Create an Amazon CloudFront distribution that refers to this S3 bucket, with the origin response event set to trigger a Lambda@Edge Node.js function to add in the securityheaders.
D. Use an Amazon S3 bucket configured for website hosting. Create an Amazon CloudFront distribution that refers to this S3 bucket. Set "Cache Based on Selected Request Headers" to "Whitelist," and add the security headers into thewhitelist.



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

**Explanation/Reference:**

**QUESTION 107**
An e-commerce company is running a web application in an AWS Elastic Beanstalk environment. In recent months, the average load of the Amazon EC2 instances has been increased to handle more traffic.
The company would like to improve the scalability and resilience of the environment. The Development team has been asked to decouple long-running tasks from the environment if the tasks can be executed asynchronously. Examples of these tasks include confirmation emails when users are registered to the platform, and processing images or videos. Also, some of the periodic tasks that are currently running within the web server should be offloaded. What is the most time-efficient and integrated way to achieve this?

A. Create an Amazon SQS queue and send the tasks that should be decoupled from the Elastic Beanstalk web server environment to the SQS queue. Create a fleet of EC2 instances under an Auto Scaling group. Use an AMI that containsthe application to process the asynchronous tasks, configure the application to listen for messages within the SQS queue, and create periodic tasks by placing those into the cron in the operating system. Create an environment variable

within the Elastic Beanstalk environment with a value pointing to the SQS queue endpoint.

B. Create a second Elastic Beanstalk worker tier environment and deploy the application to process the asynchronous tasks there. Send the tasks that should be decoupled from the original Elastic Beanstalk web server environment to theauto-generated Amazon SQS queue by the Elastic Beanstalk worker environment. Place a cron.yaml file within the root of the application source bundle for the worker environment periodic tasks. Use environment links to link the web server environment with the worker environment.

C. Create a second Elastic Beanstalk web server tier environment and deploy the application to process the asynchronous tasks. Send the tasks that should be decoupled from the original Elastic Beanstalk web server to the auto-generated Amazon SQS queue by the second Elastic Beanstalk web server tier environment. Place a cron.yaml file within the root of the application source bundle for the second web server tier environment with the necessary periodic tasks. Use environment links to link both web server environments.

D. Create an Amazon SQS queue and send the tasks that should be decoupled from the Elastic Beanstalk web server environment to the SQS queue. Create a fleet of EC2 instances under an Auto Scaling group. Install and configure theapplication to listen for messages within the SQS queue from UserData and create periodic tasks by placing those into the cron in the operating system. Create an environment variable within the Elastic Beanstalk web server environment with a value pointing to the SQS queue endpoint.

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

**Explanation/Reference:**



**QUESTION 108**
A defect was discovered in production and a new sprint item has been created for deploying a hotfix. However, any code change must go through the following steps before going into production: Scan the code for security breaches, such as password and access key leaks. Run the code through extensive, long running unit tests.
Which source control strategy should a DevOps Engineer use in combination with AWS CodePipeline to complete this process?

A. Create a hotfix tag on the last commit of the master branch. Trigger the development pipeline from the hotfix tag. Use AWS CodeDeploy with Amazon ECS to do a content scan and run unit tests. Add a manual approval stage thatmerges the hotfix tag into the master branch.

B. Create a hotfix branch from the master branch. Trigger the development pipeline from the hotfix branch. Use AWS CodeBuild to do a content scan and run unit tests. Add a manual approval stage that merges the hotfix branch into the master branch.

C. Create a hotfix branch from the master branch. Trigger the development pipeline from the hotfix branch. Use AWS Lambda to do a content scan and run unit tests. Add a manual approval stage that merges the hotfix branch into the master branch.

D. Create a hotfix branch from the master branch. Create a separate source stage for the hotfix branch in the production pipeline. Trigger the pipeline from the hotfix branch. Use AWS Lambda to do a content scan and use AWS CodeBuildto run unit tests. Add a manual approval stage that merges the hotfix branch into the master branch.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 109**
The management team at a company with a large on-premises OpenStack environment wants to move non-production workloads to AWS. An AWS Direct Connect connection has been provisioned and configured to connect the
environments. Due to contractual obligations, the production workloads must remain on-premises, and will be moved to AWS after the next contract negotiation. The company follows Center for Internet Security (CIS) standards for hardening images; this configuration was developed using the company's configuration management system.
Which solution will automatically create an identical image in the AWS environment without significant overhead?

A. Write an AWS CloudFormation template that will create an Amazon EC2 instance. Use cloud-unit to install the configuration management agent, use cfn-wait to wait for configuration management to successfully apply, and use an AWSLambda-backed custom resource to create the AMI.
B. Log in to the console, launch an Amazon EC2 instance, and install the configuration management agent. When changes are applied through the configuration management system, log in to the console and create a new AMI from theinstance.
C. Create a new AWS OpsWorks layer and mirror the image hardening standards. Use this layer as the baseline for all AWS workloads.
D. When a change is made in the configuration management system, a job in Jenkins is triggered to use the VM Import command to create an Amazon EC2 instance in the Amazon VPC. Use lifecycle hooks to launch an AWS Lambdafunction to create the AMI.



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

**Explanation/Reference:**

**QUESTION 110**
A DevOps engineer is writing an AWS CloudFormation template to stand up a web service that will run on Amazon EC2 instances in a private subnet behind an ELB Application Load Balancer. The Engineer must ensure that the service can accept requests from clients that have IPv6 addresses.
Which configuration items should the Engineer incorporate into the CloudFormation template to allow IPv6 clients to access the web service?

A. Associate an IPv6 CIDR block with the Amazon VPC and subnets where the EC2 instances will live. Create route table entries for the IPv6 network, use EC2 instance types that support IPv6, and assign IPv6 addresses to each EC2instance.
B. Replace the Application Load Balancer with a Network Load Balancer. Associate an IPv6 CIDR block with the Virtual Private Cloud (VPC) and subnets where the Network Load Balancer lives, and assign the Network Load Balancer anIPv6 Elastic IP address.
C. Assign each EC2 instance an IPv6 Elastic IP address. Create a target group and add the EC2 instances as targets. Create a listener on port 443 of the Application Load Balancer, and associate the newly created target group as thedefault target group.

D. Create a target group and add the EC2 instances as targets. Create a listener on port 443 of the Application Load Balancer. Associate the newly created target group as the default target group. Select a dual stack IP address, and createa rule in the security group that allows inbound traffic from anywhere.

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

**Explanation/Reference:**

**QUESTION 111**
A Security team is concerned that a Developer can unintentionally attach an Elastic IP address to an Amazon EC2 instance in production. No Developer should be allowed to attach an Elastic IP address to an instance. The Security team must be notified if any production server has an Elastic IP address at any time. How can this task be automated?

A. Use Amazon Athena to query AWS CloudTrail logs to check for any associate-address attempts. Create an AWS Lambda function to disassociate the Elastic IP address from the instance, and alert the Security team.
B. Attach an IAM policy to the Developers' IAM group to deny associate-address permissions. Create a custom AWS Config rule to check whether an Elastic IP address is associated with any instance tagged as production, and alert theSecurity team.
C. Ensure that all IAM groups are associated with Developers do not have associate-address permissions. Create a scheduled AWS Lambda function to check whether an Elastic IP address is associated with any instance tagged asproduction, and alert the Security team if an instance has an Elastic IP address associated with it.
D. Create an AWS Config rule to check that all production instances have the EC2 IAM roles that include deny associate-address permissions. Verify whether there is an Elastic IP address associated with any instance, and alert the Securityteam if an instance has an Elastic IP address associated with it.

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

**Explanation/Reference:**

**QUESTION 112**
A company has developed a Node.js web application which provides REST services to store and retrieve time series data. The web application is built by the Development team on company laptops, tested locally, and manually deployed to a single on-premises server, which accesses a local MySQL database. The company is starting a trial in two weeks, during which the application will undergo frequent updates based on customer feedback. The following requirements must be met:
The team must be able to reliably build, test, and deploy new updates on a daily basis, without downtime or degraded performance. The application must be able to scale to meet an unpredictable number of concurrent users during the trial.
Which action will allow the team to quickly meet these objectives?

A. Create two Amazon Lightsail virtual private servers for Node.js; one for test and one for production. Build the Node.js application using existing processes and upload it to the new Lightsail test server using the AWS CLI. Test theapplication, and if it passes all tests, upload it to the production server. During the trial, monitor the production server usage, and if needed, increase performance by upgrading the instance type.
B. Develop an AWS CloudFormation template to create an Application Load Balancer and two Amazon EC2 instances with Amazon EBS (SSD) volumes in an Auto Scaling group with rolling updates enabled. Use AWS CodeBuild to buildand test the Node.js application and store it in an Amazon S3 bucket. Use user-data scripts to install the application and the MySQL database on each EC2 instance. Update the stack to deploy new application versions.
C. Configure AWS Elastic Beanstalk to automatically build the application using AWS CodeBuild and to deploy it to a test environment that is configured to support auto scaling. Create a second Elastic Beanstalk environment forproduction. Use Amazon RDS to store data. When new versions of the applications have passed all tests, use Elastic Beanstalk 'swap cname' to promote the test environment to production.
D. Modify the application to use Amazon DynamoDB instead of a local MySQL database. Use AWS OpsWorks to create a stack for the application with a DynamoDB layer, an Application Load Balancer layer, and an Amazon EC2 instancelayer. Use a Chef recipe to build the application and a Chef recipe to deploy the application to the EC2 instance layer. Use custom health checks to run unit tests on each instance with rollback on failure.

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

**Explanation/Reference:**



**QUESTION 113**
A DevOps Engineer is developing a deployment strategy that will allow for data-driven decisions before a feature is fully approved for general availability. The current deployment process uses AWS CloudFormation and blue/green-style deployments. The development team has decided that customers should be randomly assigned to groups, rather than using a set percentage, and redirects should be avoided. What process should be followed to implement the new deployment strategy?

A. Configure Amazon Route 53 weighted records for the blue and green stacks, with 50% of traffic configured to route to each stack.
B. Configure Amazon CloudFront with an AWS Lambda@Edge function to set a cookie when CloudFront receives a request. Assign the user to a version A or B, and configure the web server to redirect to version A or B.
C. Configure Amazon CloudFront with an AWS Lambda@Edge function to set a cookie when CloudFront receives a request. Assign the user to a version A or B, then return the corresponding version to the viewer.
D. Configure Amazon Route 53 with an AWS Lambda function to set a cookie when Amazon CloudFront receives a request. Assign the user to version A or B, then return the corresponding version to the viewer.

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

**Explanation/Reference:**

**QUESTION 114**
A company is testing a web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company uses a blue/green deployment process with immutable instances when deploying new software.
During testing, users are being automatically logged out of the application at random times. Testers also report that, when a new version of the application is deployed, all users are logged out. The Development team needs a solution to ensure users remain logged in across scaling events and application deployments. What is the MOST efficient way to ensure users remain logged in?

A. Enable smart sessions on the load balancer and modify the application to check for an existing session.
B. Enable session sharing on the load balancer and modify the application to read from the session store.
C. Store user session information in an Amazon S3 bucket and modify the application to read session information from the bucket.
D. Modify the application to store user session information in an Amazon ElastiCache cluser.

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

**Explanation/Reference:**



**QUESTION 115**
A company is reviewing its IAM policies. One policy written by the DevOps Engineer has been flagged as too permissive. The policy is used by an AWS Lambda function that issues a stop command to Amazon EC2 instances tagged with `Environment: NonProduction` over the weekend. The current policy is:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    }
  ]
}
```

What changes should the Engineer make to achieve a policy of least permission? (Choose three.)

A. Add the following conditional expression:

```
"Condition": {
  "StringEquals": {
    "aws:principaltype": "lambda.amazonaws.com"
  }
}
```

B. Change `"Resource": "*"` to `"Resource": "arn:aws:ec2:*:*:instance/*"`

C. Add the following conditional expression:

```
"Condition": {
  "StringNotEquals": {
    "ec2:ResourceTag/Environment": "Production"
  }
}
```



D. Add the following conditional expression:

```
"Condition": {
  "StringEquals": {
    "ec2:ResourceTag/Environment": "NonProduction"
  }
}
```

E. Change `"Action": "ec2:*"` to `"Action": "ec2:StopInstances"`

F.

Add the following conditional expression:

```
"Condition" :  {
  "DateGreaterThan" : {
    "aws:CurrentTime" : "${aws:DateTime:Friday}"
  },
  "DateLessThan": {
    "aws:CurrentTime" : "${aws:DateTime:Monday}"
  }
}
```

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

**Explanation/Reference:**

**QUESTION 116**
A web application for healthcare services runs on Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. A DevOps Engineer must create a mechanism in which an EC2 instance can be taken out of production so its system logs can be analyzed for issues to quickly troubleshot problems on the web tier. How can the Engineer accomplish this task while ensuring availability and minimizing downtime?

A. Implement EC2 Auto Scaling groups cooldown periods. Use EC2 instance metadata to determine the instance state, and an AWS Lambda function to snapshot Amazon EBS volumes to preserve system logs.
B. Implement Amazon CloudWatch Events rules. Create an AWS Lambda function that can react to an instance termination to deploy the CloudWatch Logs agent to upload the system and access logs to Amazon S3 for analysis.
C. Terminate the EC2 instances manually. The Auto Scaling service will upload all log information to CloudWatch Logs for analysis prior to instance termination.
D. Implement EC2 Auto Scaling groups with lifecycle hooks. Create an AWS Lambda function that can modify an EC2 instance lifecycle hook into a standby state, extract logs from the instance through a remote script execution, and placethem in an Amazon S3 bucket for analysis.

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

**Explanation/Reference:**

**QUESTION 117**
A Development team creates a build project in AWS CodeBuild. The build project invokes automated tests of modules that access AWS services. Which of the following will enable the tests to run the MOST securely?

A. Generate credentials for an IAM user with a policy attached to allow the actions on AWS services. Store credentials as encrypted environment variables for the build project. As part of the build script, obtain the credentials to run theintegration tests.
B. Have CodeBuild run only the integration tests as a build job on a Jenkins server. Create a role that has a policy attached to allow the actions on AWS services. Generate credentials for an IAM user that is allowed to assume the role.Configure the credentials as secrets in Jenkins, and allow the build job to use them to run the integration tests.
C. Create a service role in IAM to be assumed by CodeBuild with a policy attached to allow the actions on AWS services. Configure the build project to use the role created.
D. Use AWS managed credentials. Encrypt the credentials with AWS KMS. As part of the build script, decrypt with AWS KMS and use these credentials to run the integration tests.

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

**Explanation/Reference:**



**QUESTION 118**
A retail company wants to use AWS Elastic Beanstalk to host its online sales website running on Java. Since this will be the production website, the CTO has the following requirements for the deployment strategy:
Zero downtime. While the deployment is ongoing, the current Amazon EC2 instances in service should remain in service. No deployment or any other action should be performed on the EC2 instances because they serve production traffic.
A new fleet of instances should be provisioned for deploying the new application version.
Once the new application version is deployed successfully in the new fleet of instances, the new instances should be placed in service and the old ones should be removed.
The rollback should be as easy as possible. If the new fleet of instances fail to deploy the new application version, they should be terminated and the current instances should continue serving traffic as normal.
The resources within the environment (EC2 Auto Scaling group, Elastic Load Balancing, Elastic Beanstalk DNS CNAME) should remain the same and no DNS change should be made.
Which deployment strategy will meet the requirements?

A. Use rolling deployments with a fixed amount of one instance at a time and set the healthy threshold to OK.
B. Use rolling deployments with additional batch with a fixed amount of one instance at a time and set the healthy threshold to OK.
C. launch a new environment and deploy the new application version there, then perform a CNAME swap between environments.
D. Use immutable environment updates to meet all the necessary requirements.

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

**Explanation/Reference:**

**QUESTION 119**
A company is using AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline to deploy applications automatically to an Amazon EC2 instance. A DevOps Engineer needs to perform a security assessment scan of the operating system on every application deployment to the environment. How should this be automated?

A. Use Amazon CloudWatch Events to monitor for Auto Scaling event notifications of new instances and configure CloudWatch Events to trigger an Amazon Inspector scan.
B. Use Amazon CloudWatch Events to monitor for AWS CodeDeploy notifications of a successful code deployment and configure CloudWatch Events to trigger an Amazon Inspector scan.
C. Use Amazon CloudWatch Events to monitor for CodePipeline notifications of a successful code deployment and configure CloudWatch Events to trigger an AWS X-Ray scan.
D. Use Amazon Inspector as a CodePipeline task after the successful use of CodeDeploy to deploy the code to the systems.



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

**Explanation/Reference:**

**QUESTION 120**
A company that uses electronic health records is running a fleet of Amazon EC2 instances with an Amazon Linux operating system. As part of patient privacy requirements, the company must ensure continuous compliance for patches for operating system and applications running on the EC2 instances.
How can the deployments of the operating system and application patches be automated using a default and custom repository?

A. Use AWS Systems Manager to create a new patch baseline including the custom repository. Execute the AWS-RunPatchBaseline document using the run command to verify and install patches.
B. Use AWS Direct Connect to integrate the corporate repository and deploy the patches using Amazon CloudWatch scheduled events, then use the CloudWatch dashboard to create reports.
C. Use yum-config-manager to add the custom repository under /etc/yum.repos.d and run yum-config-manager-enable to activate the repository.
D. Use AWS Systems Manager to create a new patch baseline including the corporate repository. Execute the AWS-AmazonLinuxDefaultPatchBaseline document using the run command to verify and install patches.

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

**Explanation/Reference:**

**QUESTION 121**
A company using AWS CodeCommit for source control wants to automate its continuous integration and continuous deployment pipeline on AWS in its development environment. The company has three requirements:
1. There must be a legal and a security review of any code change to make sure sensitive information is not leaked through the source code.
2. Every change must go through unit testing.
3. Every change must go through a suite of functional testing to ensure functionality.
In addition, the company has the following requirements for automation:
1. Code changes should automatically trigger the CI/CD pipellline.
2. Any failure in the pipeline should notify devops-admin@xyz.com.
3. There must be an approval to stage the assets to Amazon S3 after tests have been performed.
What should a DevOps Engineer do to meet all of these requirements while following CI/CD best practices?

A. Commit to the development branch and trigger AWS CodePipeline from the development branch. Make an individual stage in CodePipeline for security review, unit tests, functional tests, and manual approval. Use Amazon CloudWatchmetrics to detect changes in pipeline stages and Amazon SES for emailing devops-admin@xyz.com.
B. Commit to mainline and trigger AWS CodePipeline from mainline. Make an individual stage in CodePipeline for security review, unit tests, functional tests, and manual approval. Use AWS CloudTrail logs to detect changes in pipelinestages and Amazon SNS for emailing devops-admin@xyz.com.
C. Commit to the development branch and trigger AWS CodePipeline from the development branch. Make an individual stage in CodePipeline for security review, unit tests, functional tests, and manual approval. Use Amazon CloudWatchEvents to detect changes in pipeline stages and Amazon SNS for emailing devops-admin@xyz.com.
D. Commit to mainline and trigger AWS CodePipeline from mainline. Make an individual stage in CodePipeline for security review, unit tests, functional tests, and manual approval. Use Amazon CloudWatch Events to detect changes inpipeline stages and Amazon SES for emailing devops-admin@xyz.com.

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

**Explanation/Reference:**

**QUESTION 122**
A DevOps Engineer uses Docker container technology to build an image-analysis application. The application often sees spikes in traffic. The Engineer must

automatically scale the application in response to customer demand while maintaining cost effectiveness and minimizing any impact on availability.
What will allow the FASTEST response to spikes in traffic while fulfilling the other requirements?

A. Create an Amazon ECS cluster with the container instances in an Auto Scaling group. Configure the ECS service to use Service Auto Scaling. Set up Amazon CloudWatch alarms to scale the ECS service and cluster.
B. Deploy containers on an AWS Elastic Beanstalk Multicontainer Docker environment. Configure Elastic Beanstalk to automatically scale the environment based on Amazon CloudWatch metrics.
C. Create an Amazon ECS cluster using Spot instances. Configure the ECS service to use Service Auto Scaling. Set up Amazon CloudWatch alarms to scale the ECS service and cluster.
D. Deploy containers on Amazon EC2 instances. Deploy a container scheduler to schedule containers onto EC2 instances. Configure EC2 Auto Scaling for EC2 instances based on available Amazon CloudWatch metrics.

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

**Explanation/Reference:**

**QUESTION 123**
A DevOps Engineer is building a multi-stage pipeline with AWS CodePipeline to build, verify, stage, test, and deploy an application. There is a manual approval stage required between the test and deploy stages. The development team uses a team chat tool with webhook support.
How can the Engineer configure status updates for pipeline activity and approval requests to post to the chat tool?

A. Create an AWS CloudWatch Logs subscription that filters on "detail-type": "CodePipeline Pipeline Execution State Change." Forward that to an Amazon SNS topic. Add the chat webhook URL to the SNS topic as a subscriber andcomplete the subscription validation.
B. Create an AWS Lambda function that is triggered by the updating of AWS CloudTrail events. When a "CodePipeline Pipeline Execution State Change" event is detected in the updated events, send the event details to the chat webhookURL.
C. Create an AWS CloudWatch Events rule that filters on "CodePipeline Pipeline Execution State Change." Forward that to an Amazon SNS topic. Subscribe an AWS Lambda function to the Amazon SNS topic and have it forward theevent to the chat webhook URL.
D. Modify the pipeline code to send event details to the chat webhook URL at the end of each stage. Parameterize the URL so each pipeline can send to a different URL based on the pipeline environment.

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

**Explanation/Reference:**

**QUESTION 124**
A company is beginning to move to the AWS Cloud. Internal customers are classified into two groups according to their AWS skills: beginners and experts. The DevOps Engineer needs to build a solution to allow beginners to deploy a restricted set of AWS architecture blueprints expresses as AWS CloudFormation templates. Deployment should only be possible on predetermined Virtual Private Clouds (VPCs). However, expert users should be able to deploy blueprints without constraints. Experts should also be able to access other AWS services, as needed. How can the Engineer implement a solution to meet these requirements with the LEAST amount of overhead?

A. Apply constraints to the parameters in the templates, limiting the VPCs available for deployments. Store the templates on Amazon S3. Create an IAM group for beginners and give them access to the templates and CloudFormation.Create a separate group for experts, giving them access to the templates, CloudFormation, and other AWS services.
B. Store the templates on Amazon S3. Use AWS Service Catalog to create a portfolio of products based on those templates. Apply template constraints to the products with rules limiting VPCs available for deployments. Create an IAMgroup for beginners giving them access to the portfolio. Create a separate group for experts giving them access to the templates, CloudFormation, and other AWS services.
C. Store the templates on Amazon S3. Use AWS Service Catalog to create a portfolio of products based on those templates. Create an IAM role restricting VPCs available for creation of AWS resources. Apply a launch constraint to theproducts using this role. Create an IAM group for beginners giving them access to the portfolio. Create a separate group for experts giving them access to the portfolio and other AWS services.
D. Create two templates for each architecture blueprint where only one of them limits the VPC available for deployments. Store the templates in Amazon DynamoDB. Create an IAM group for beginners giving them access to the constrainedtemplates and CloudFormation. Create a separate group for experts giving them access to the unconstrained templates, CloudFormation, and other AWS services.



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

**Explanation/Reference:**

**QUESTION 125**
A DevOps Engineer encountered the following error when attempting to use an AWS CloudFormation template to create an Amazon ECS cluster:
An error occurred (InsufficientCapabilitiesException) when calling the CreateStack operation.
What caused this error and what steps need to be taken to allow the Engineer to successfully execute the AWS CloudFormation template?

A. The AWS user or role attempting to execute the CloudFormation template does not have the permissions required to create the resources within the template. The Engineer must review the user policies and add any permissions neededto create the resources and then rerun the template execution.
B. The AWS CloudFormation service cannot be reached and is not capable of creating the cluster. The Engineer needs to confirm that routing and firewall rules are not preventing the AWS CloudFormation script from communicating withthe AWS service endpoints, and then rerun the template execution.
C. The CloudFormation execution was not granted the capability to create IAM resources. The Engineer needs to provide CAPABILITY_IAM and CAPABILITY_NAMED_IAM as capabilities in the CloudFormation execution parameters or provide the capabilities in the AWS Management Console.
D. CloudFormation is not capable of fulfilling the request of the specified resources in the current AWS Region. The Engineer needs to specify a new region and

rerun the template.

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

**Explanation/Reference:**
Reference: https://github.com/awslabs/serverless-application-model/issues/51

**QUESTION 126**
A retail company is currently hosting a Java-based application in its on-premises data center. Management wants the DevOps Engineer to move this application to AWS. Requirements state that while keeping high availability, infrastructure management should be as simple as possible. Also, during deployments of new application versions, while cost is an important metric, the Engineer needs to ensure that at least half of the fleet is available to handle user traffic. What option requires the LEAST amount of management overhead to meet these requirements?

A. Create an AWS CodeDeploy deployment group and associate it with an Auto Scaling group configured to launch instances across subnets in different Availability Zones. Configure an in-place deployment with a CodeDeploy.HalfAtAtimeconfiguration for application deployments.
B. Create an AWS Elastic Beanstalk Java-based environment using Auto Scaling and load balancing. Configure the network setting for the environment to launch instances across subnets in different Availability Zones. Use "Rolling withadditional batch" as a deployment strategy with a batch size of 50%.
C. Create an AWS CodeDeploy deployment group and associate it with an Auto Scaling group configured to launch instances across subnets in different Availability Zones. Configure an in-place deployment with a custom deploymentconfiguration with the MinimumHealthyHosts option set to type FLEET_PERCENT and a value of 50.
D. Create an AWS Elastic Beanstalk Java-based environment using Auto Scaling and load balancing. Configure the network options for the environment to launch instances across subnets in different Availability Zones. Use "Rolling" as adeployment strategy with a batch size of 50%.

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

**Explanation/Reference:**

**QUESTION 127**
A global company with distributed Development teams built a web application using a microservices architecture running on Amazon ECS. Each application service is independent and runs as a service in the ECS cluster. The container build files and source code reside in a private GitHub source code repository. Separate ECS clusters exist for development, testing, and production environments.
Developers are required to push features to branches in the GitHub repository and then merge the changes into an environment-specific branch (development, test, or production). This merge needs to trigger an automated pipeline to run a build and a deployment to the appropriate ECS cluster.
What should the DevOps Engineer recommend as an automated solution to these requirements?

A. Create an AWS CloudFormation stack for the ECS cluster and AWS CodePipeline services. Store the container build files in an Amazon S3 bucket. Use a post-commit hook to trigger a CloudFormation stack update that deploys the ECScluster. Add a task in the ECS cluster to build and push images to Amazon ECR, based on the container build files in S3.
B. Create a separate pipeline in AWS CodePipeline for each environment. Trigger each pipeline based on commits to the corresponding environment branch in GitHub. Add a build stage to launch AWS CodeBuild to create the containerimage from the build file and push it to Amazon ECR. Then add another stage to update the Amazon ECS task and service definitions in the appropriate cluster for that environment.
C. Create a pipeline in AWS CodePipeline. Configure it to be triggered by commits to the master branch in GitHub. Add a stage to use the Git commit message to determine which environment the commit should be applied to, then call thecreate-image Amazon ECR command to build the image, passing it to the container build file. Then add a stage to update the ECS task and service definitions in the appropriate cluster for that environment.
D. Create a new repository in AWS CodeCommit. Configure a scheduled project in AWS CodeBuild to synchronize the GitHub repository to the new CodeCommit repository. Create a separate pipeline for each environment triggered bychanges to the CodeCommit repository. Add a stage using AWS Lambda to build the container image and push to Amazon ECR. Then add another stage to update the ECS task and service definitions in the appropriate cluster for that environment.

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

**Explanation/Reference:**



**QUESTION 128**
For auditing, analytics, and troubleshooting purposes, a DevOps Engineer for a data analytics application needs to collect all of the application and Linux system logs from the Amazon EC2 instances before termination. The company, on average, runs 10,000 instances in an Auto Scaling group. The company requires the ability to quickly find logs based on instance IDs and date ranges. Which is the MOST cost-effective solution?

A. Create an EC2 Instance-terminate Lifecycle Action on the group, write a termination script for pushing logs into Amazon S3, and trigger an AWS Lambda function based on S3 PUT to create a catalog of log files in an Amazon DynamoDB table with the primary key being Instance ID and sort key being Instance Termination Date.
B. Create an EC2 Instance-terminate Lifecycle Action on the group, write a termination script for pushing logs into Amazon CloudWatch Logs, create a CloudWatch Events rule to trigger an AWS Lambda function to create a catalog of log files in an Amazon DynamoDB table with the primary key being Instance ID and sort key being Instance Termination Date.
C. Create an EC2 Instance-terminate Lifecycle Action on the group, create an Amazon CloudWatch Events rule based on it to trigger an AWS Lambda function for storing the logs in Amazon S3, and create a catalog of log files in an Amazon DynamoDB table with the primary key being Instance ID and sort key being Instance Termination Date.
D. Create an EC2 Instance-terminate Lifecycle Action on the group, push the logs into Amazon Kinesis Data Firehose, and select Amazon ES as the destination for providing storage and search capability.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 129**
A DevOps Engineer manages a large commercial website that runs on Amazon EC2. The website uses Amazon Kinesis Data Streams to collect and process web logs. The Engineer manages the Kinesis consumer application, which also runs on EC2. Spikes of data cause the Kinesis consumer application to fall behind, and the streams drop records before they can be processed. What is the FASTEST method to improve stream handling?

A. Modify the Kinesis consumer application to store the logs durably in amazon S3. Use Amazon EMR to process the data directly on S3 to derive customer insights and store the results in S3.
B. Horizontally scale the Kinesis consumer application by adding more EC2 instances based on the GetRecord.IteratorAgeMiliseconds Amazon CloudWatch metric. Increase the Kinesis Data Streams retention period.
C. Convert the Kinesis consumer application to run as an AWS Lambda function. Configure the Kinesis Data Streams as the event source for the Lambda function to process the data streams.
D. Increase the number of shards in the Kinesis Data Streams to increase the overall throughput so that the consumer processes data faster.

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



**Explanation/Reference:**

**QUESTION 130**
A DevOps Engineer must automate a weekly process of identifying unnecessary permissions on a per-user basis, across all users in an AWS account. This process should evaluate the permissions currently granted to each user by examining the user's attached IAM access policies compared to the permissions the user has actually used in the past 90 days. Any differences in the comparison would indicate that the user has more permissions than are required. A report of the deltas should be sent to the Information Security team for further review and IAM user access policy revisions, as required. Which solution is fully automated and will produce the MOST detailed deltas report?

A. Create an AWS Lambda function that calls the IAM Access Advisor API to pull service permissions granted on a user-by-user basis for all users in the AWS account. Ensure that Access Advisor is configured with a tracking period of 90days. Invoke the Lambda function using an Amazon CloudWatch Events rule on a weekly schedule. For each record, by user, by service, if the Access Advisor Last Accesses field indicates a day count instead of "Not accesses in the tracking period," this indicates a delta compared to what is in the user's currently attached access polices. After Lambda has iterated through all users in the AWS account, configure it to generate a report and send the report using Amazon SES.
B. Configure an AWS CloudTrail trail that spans all AWS Regions and all read/write events, and point this trail to an Amazon S3 bucket. Create Amazon Athena table and specify the S3 bucket ARN in the CREATE TABLE query. Create anAWS Lambda function that accesses the Athena table using the SDK, which performs a SELECT, ensuring that the WHERE clause includes userIdentity, eventName, and eventTime. Compare the results against the user's currently

attached IAM access policies to determine any deltas. Configure an Amazon CloudWatch Events schedule to automate this process to run once a week. Configure Amazon SES to send a consolidated report to the Information Security team.

C. Configure VPC Flow Logs on all subnets across all VPCs in all regions to capture user traffic across the entire account. Ensure that all logs are being sent to a centralized Amazon S3 bucket, so all flow logs can be consolidated andaggregated. Create an AWS Lambda function that is triggered once a week by an Amazon CloudWatch Events schedule. Ensure that the Lambda function parses the flow log files for the following information: IAM user ID, subnet ID, VPC ID, Allow/Reject status per API call, and service name. Then have the function determine the deltas on a user-by-user basis. Configure the Lambda function to send the consolidated report using Amazon SES.

D. Create an Amazon ES cluster and note its endpoint URL, which will be provided as an environment variable into a Lambda function. Configure an Amazon S3 event on a AWS CloudTrail trail destination S3 bucket and ensure that theevent is configured to send to a Lambda function. Create the Lambda function to consume the events, parse the input from JSON, and transform it to an Amazon ES document format. POST the documents to the Amazon ES cluster's endpoint by way of the passed-in environment variable. Make sure that the proper indexing exists in Amazon ES and use Apache Lucene queries to parse the permissions on a user-by-user basis. Export the deltas into a report and have Amazon ES send the reports to the Information Security team using Amazon SES every week.

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

**Explanation/Reference:**



**QUESTION 131**
A company is hosting a web application in an AWS Region. For disaster recovery purposes, a second region is being used as a standby. Disaster recovery requirements state that session data must be replicated between regions in near-real time and 1% of requests should route to the secondary region to continuously verify system functionality. Additionally, if there is a disruption in service in the main region, traffic should be automatically routed to the secondary region, and the secondary region must be able to scale up to handle all traffic. How should a DevOps Engineer meet these requirements?

A. In both regions, deploy the application on AWS Elastic Beanstalk and use Amazon DynamoDB global tables for session data. Use an Amazon Route 53 weighted routing policy with health checks to distribute the traffic across the regions.

B. In both regions, launch the application in Auto Scaling groups and use DynamoDB for session data. Use a Route 53 failover routing policy with health checks to distribute the traffic across the regions.

C. In both regions, deploy the application in AWS Lambda, exposed by Amazon API Gateway, and use Amazon RDS PostgreSQL with cross-region replication for session data. Deploy the web application with client-side logic to call the APIGateway directly.

D. In both regions, launch the application in Auto Scaling groups and use DynamoDB global tables for session data. Enable an Amazon CloudFront weighted distribution across regions. Point the Amazon Route 53 DNS record at theCloudFront distribution.

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

**Explanation/Reference:**

**QUESTION 132**
A DevOps Engineer manages an application that has a cross-region failover requirement. The application stores its data in an Amazon Aurora on Amazon RDS database in the primary region with a read replica in the secondary region. The application uses Amazon Route 53 to direct customer traffic to the active region. Which steps should be taken to MINIMIZE downtime if a primary database fails?

A. Use Amazon CloudWatch to monitor the status of the RDS instance. In the event of a failure, use a CloudWatch Events rule to send a short message service (SMS) to the Systems Operator using Amazon SNS. Have the SystemsOperator redirect traffic to an Amazon S3 static website that displays a downtime message. Promote the RDS read replica to the master. Confirm that the application is working normally, then redirect traffic from the Amazon S3 website to the secondary region.
B. Use RDS Event Notification to publish status updates to an Amazon SNS topic. Use an AWS Lambda function subscribed to the topic to monitor database health. In the event of a failure, the Lambda function promotes the read replica,then updates Route 53 to redirect traffic from the primary region to the secondary region.
C. Set up an Amazon CloudWatch Events rule to periodically invoke an AWS Lambda function that checks the health of the primary database. If a failure is detected, the Lambda function promotes the read replica. Then, update Route 53to redirect traffic from the primary to the secondary region.
D. Set up Route 53 to balance traffic between both regions equally. Enable the Aurora multi-master option, then set up a Route 53 health check to analyze the health of the databases. Configure Route 53 to automatically direct all traffic tothe secondary region when a primary database fails.



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

**Explanation/Reference:**

**QUESTION 133**
A company is running an application on Amazon EC2 instances behind an ELB Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones.

After a recent application update, users are getting HTTP 502 Bad Gateway errors from the application URL. The DevOps Engineer cannot analyze the problem because Auto Scaling is terminating all EC2 instances shortly after launch for being unhealthy.

What steps will allow the DevOps Engineer access to one of the unhealthy instances to troubleshoot the deployed application?

A. Create an image from the terminated instance and create a new instance from that image. The Application team can then log into the new instance.
B. As soon as a new instance is created by AutoScaling, put the instance into a `Standby` state as this will prevent the instance from being terminated.
C. Add a lifecycle hook to your Auto Scaling group to move instances in the `Terminating` state to the `Terminating:Wait` state.

D. Edit the Auto Scaling group to enable termination protection as this will protect unhealthy instances from being terminated.

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

**Explanation/Reference:**

**QUESTION 134**
An application is running on Amazon EC2. It has an attached IAM role that is receiving an AccessDenied error while trying to access a SecureString parameter resource in the AWS Systems Manager Parameter Store. The SecureString parameter is encrypted with a customer-managed Customer Master Key (CMK),

What steps should the DevOps Engineer take to grant access to the role while granting least privilege? (Select three.)

A. Set `ssm:GetParamter` for the parameter resource in the instance role's IAM policy.
B. Set `kms:Decrypt` for the instance role in the customer-managed CMK policy.
C. Set `kms:Decrypt` for the customer-managed CMK resource in the role's IAM policy.
D. Set `ssm:DecryptParameter` for the parameter resource in the instance role IAM policy.
E. Set `kms:GenerateDataKey` for the user on the AWS managed SSM KMS key.
F. Set `kms:Decrypt` for the parameter resource in the customer-managed CMK policy.



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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-paramstore-access.html

**QUESTION 135**
An Application team is refactoring one of its internal tools to run in AWS instead of on-premises hardware. All of the code is currently written in Python and is standalone. There is also no external state store or relational database to be queried.

Which deployment pipeline incurs the LEAST amount of changes between development and production?

A. Developers should use Docker for local development. When dependencies are changed and a new container is ready, use AWS CodePipeline and AWS CodeBuild to perform functional tests and then upload the new container to Amazon ECR. Use AWS CloudFormation with the custom container to deploy the new Amazon ECS.
B. Developers should use Docker for local development. Use AWS SMS to import these containers as AMIs for Amazon EC2 whenever dependencies are

updated. Use AWS CodePipeline to test new code changes against the Auto Scaling group.

C. Developers should use their native Python environment. When Dependencies are changed and a new container is ready, use AWS CodePipeline and AWS CodeBuild to perform functional tests and then upload the new container to the Amazon ECR. Use AWS CloudFormation with the custom container to deploy the new Amazon ECS.

D. Developers should use their native Python environment. When Dependencies are changed and a new code is ready, use AWS CodePipeline and AWS CodeBuild to perform functional tests and then upload the new container to the Amazon ECR. Use CodePipeline and CodeBuild with the custom container to test new code changes inside AWS Elastic Beanstalk.

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

**Explanation/Reference:**

**QUESTION 136**
A company is using an AWS CodeBuild project to build and package an application. The packages are copied to a shared Amazon S3 bucket before being deployed across multiple AWS accounts.



The buildspec.yml file contains the following:

```
version: 0.2
phases:
  build:
    commands:
      - go build -o myapp
  post_build:
    commands:
      - aws s3 cp --acl authenticated-read myapp s3://artifacts/
```

The DevOps Engineer has noticed that anybody with an AWS account is able to download the artifacts.

What steps should the DevOps Engineer take to stop this?

A. Modify the post_build to command to use `–-acl public-read` and configure a bucket policy that grants read access to the relevant AWS accounts only.

B. Configure a default ACL for the S3 bucket that defines the set of authenticated users as the relevant AWS accounts only and grants read-only access.

C. Create an S3 bucket policy that grants read access to the relevant AWS accounts and denies read access to the principal “*”

D. Modify the `post_build` command to remove `–-acl authenticated-read` and configure a bucket policy that allows read access to the relevant AWS accounts only.

**Correct Answer:** A

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

**Explanation/Reference:**

**QUESTION 137**
A web application has been deployed using an AWS Elastic Beanstalk application The Application Developers are concerned that they are seeing high latency in two different areas of the application:

- HTTP client requests to a third-party API
- MySQL client library queries to an Amazon RDS database

A DevOps Engineer must gather trace data to diagnose the issues.

Which steps will gather the trace information with the LEAST amount of changes and performance impacts to the application?

A. Add additional logging to the application code. Use the Amazon CloudWatch agent to stream the application logs into Amazon Elasticsearch Service. Query the log data in Amazon ES.
B. Instrument the application to use the AWS X-Ray SDK. Post trace data to an Amazon Elasticsearch Service cluster. Query the trace data for calls to the HTTP client and the MySQL client.
C. On the AWS Elastic Beanstalk management page for the application, enable the AWS X-Ray daemon. View the trace data in the X-Ray console.
D. Instrument the application using the AWS X-Ray SDK. On the AWS Elastic Beanstalk management page for the application, enable the X-Ray daemon. View the trace data in the X-Ray console.

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

**Explanation/Reference:**
Reference https://docs.aws.amazon.com/xray/latest/devguide/xray-gettingstarted.html

**QUESTION 138**
An Information Security policy requires that all publicly accessible systems be patched with critical OS security patches within 24 hours of a patch release. All instances are tagged with the Patch Group key set to 0. Two new AWS Systems Manager patch baselines for Windows and Red Hat Enterprise Linux (RHEL) with zero-day delay for security patches of critical severity were created with an auto-approval rule. Patch Group 0 has been associated with the new patch baselines.

Which two steps will automate patch compliance and reporting? (Select TWO.)

A. Create an AWS Systems Manager Maintenance Window and add a target with Patch Group 0. Add a task that runs the AWS-InstallWindowsUpdates document with a daily schedule.
B. Create an AWS Systems Manager Maintenance Window with a daily schedule and add a target with Patch Group 0. Add a task that runs the AWS-RunPatchBaseline document with the `Install` action.
C. Create an AWS Systems Manager State Manager configuration. Associate the AWS-RunPatchBaseline task with the configuration and add a target with Patch Group 0.
D. Create an AWS Systems Manager Maintenance Window and add a target with Patch Group 0. Add a task that runs the AWS-ApplyPatchBaseline document with a daily schedule.
E. Use the AWS Systems Manager Run Command to associate the AWS-ApplyPatchBaseline document with instances tagged with Patch Group 0.

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

**Explanation/Reference:**
Reference https://aws.amazon.com/blogs/mt/patching-your-windows-ec2-instances-using-aws-systems-manager-patch-manager/

**QUESTION 139**
A Security team requires all Amazon EBS volumes that are attached to an Amazon EC2 instance to have AWS Key Management Service (AWS KMS) encryption enabled. If encryption is not enabled, the company's policy requires the EBS volume to be detached and deleted. A DevOps Engineer must automate the detection and deletion of unencrypted EBS volumes.



Which method should the Engineer use to accomplish this with the LEAST operational effort?

A. Create an Amazon CloudWatch Events rule that invokes an AWS Lambda function when an EBS volume is created. The Lambda function checks the EBS volume for encryption. If encryption is not enabled and the volume is attached to an instance, the function deletes the volume.
B. Create an AWS Lambda function to describe all EBS volumes in the region and identify volumes that are attached to an EC2 instance without encryption enabled. The function then deletes all non-compliant volumes. The AWS Lambda function is invoked every 5 minutes by an Amazon CloudWatch Events scheduled rule.
C. Create a rule in AWS Config to check for unencrypted and attached EBS volumes. Subscribe an AWS Lambda function to the Amazon SNS topic that AWS Config sends change notifications to. The Lambda function checks the change notification and deletes any EBS volumes that are non-compliant.
D. Launch an EC2 instance with an IAM role that has permissions to describe and delete volumes. Run a script on the EC2 instance every 5 minutes to describe all EBS volumes in all regions and identify volumes that are attached without encryption enabled. The script then deletes those volumes.

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

**Explanation/Reference:**

**QUESTION 140**
A company wants to implement a CI/CD pipeline for building and testing its mobile apps. A DevOps Engineer has been given the following requirements:

- Use AWS CodePipeline to orchestrate the workflow.
- Test the application on real devices.
- Trigger a notification.
- Stage the application binary on a production bucket in a different account.
- Make the application binary publicly accessible.

Which sequence of actions should the Engineer perform in the pipeline to meet the requirements?

A. Use AWS CodeCommit as the code source and AWS CodeDeploy to compile and package the application. Use CodeDeploy to deploy the application binary to an AWS Lambda function for testing. Use a third-party library on AWS Lambda to simulate the device platform. Allow a Lambda role to upload to the production Amazon S3 bucket. Make the binary publicly accessible. Trigger notifications using Amazon SNS.
B. Use GitHub as the code source and AWS Lambda to compile and package the application. Use another Lambda function to run unit tests and deliver the application binary to a development bucket. Use the binary from the development bucket and install the application on a personal device for testing. Deliver the binary to the production bucket after approval. Trigger notifications using Amazon SNS.
C. Use an Amazon S3 bucket as the code source and AWS CodeBuild to compile and package the application. Use AWS CodeDeploy to deploy the application binary to a device farm for testing. Deliver the binary to the production S3 bucket. Use an S3 bucket policy to allow public read on the production S3 bucket. Trigger notifications using an Amazon CloudWatch Events rule with Amazon SNS.
D. Use AWS CodeCommit as the code source and AWS CodeBuild to compile and package the application. Invoke an AWS Lambda function that uploads the application binary to a device farm for testing. Deliver the binary to the production Amazon S3 bucket. Use an S3 bucket policy to allow public read on the production S3 bucket. Trigger notifications by using an Amazon CloudWatch Events rule.

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

**Explanation/Reference:**

**QUESTION 141**
A DevOps Engineer is reviewing a system that uses Amazon EC2 instances in an Auto Scaling group. This system uses a configuration management tool that runs locally on each EC2 instance. Because of the volatility of the application load, new instances must be fully functional within 3 minutes of entering a running state. Current setup tasks include:

- Installing the configuration management agent – 2 minutes
- Installing the application framework – 15 minutes

- Copying configuration data from Amazon S3 – 2 minutes
- Running the configuration management agent to configure instances – 1 minute
- Deploying the application code from Amazon S3 – 2 minutes

How should the Engineer set up system so it meets the launch time requirement?

A. Trigger an AWS Lambda function from an Amazon CloudWatch Events rule when a new EC2 instance launches. Have the function install the configuration management agent and the application framework, pull configuration data from Amazon S3, run the agent to configure the instance, and deploy the application from S3.
B. Write a bootstrap script to install the configuration management agent, install and the application framework, pull configuration data from Amazon S3, run the agent to configure the instance, and deploy the application from S3.
C. Build a custom AMI that includes the configuration management agent and application framework. Write a bootstrap script to pull configuration data from Amazon S3, run the agent to configure the instance, and deploy the application from S3.
D. Build a custom AMI that includes the configuration management agent, application framework, and configuration data. Write a bootstrap script to run the agent to configure the instance and deploy the application from Amazon S3.

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

**Explanation/Reference:**



**QUESTION 142**
The resources for a business-critical, three-tier web application are expressed in a series of AWS CloudFormation templates. The application is using Amazon RDS for data and Amazon ElastiCache for session state. Users have reported degraded performance in the application. A DevOps Engineer notices that the T2 instance type is being used for the application tier and CPU usage is at 100% in Amazon CloudWatch.

What process should the Engineer follow to restore operations with the LEAST amount of disruption to the end users?

A. Write a new CloudFormation template to include Amazon CloudFront in the environment, launch the stack, and update the Amazon Route 53 A record
B. Launch a new CloudFormation stack for the application tier using the M4 instance type, run acceptance tests against the new stack, and update the Amazon Route 53 A record
C. Update the CloudFormation stack for the application tier using the T2 Unlimited option, run acceptance tests against the new stack, and update the Amazon Route 53 A record
D. Launch a new CloudFormation stack for all tiers of the application in a different region, run acceptance tests against the new stack, and update the Amazon Route 53 A record

**Correct Answer:** B

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

**Explanation/Reference:**

**QUESTION 143**
A company has developed an AWS Lambda function that handles orders received through an API. The company is using AWS CodeDeploy to deploy the Lambda function as the final stage of a CI/CD pipeline.

A DevOps Engineer has noticed there are intermittent failures of the ordering API for a few seconds after deployment. After some investigation, the DevOps Engineer believes the failures are due to database changes not having fully propagated before the lambda function begins executing.

How should the DevOps Engineer overcome this?

A. Add a BeforeAllowTraffic hook to the AppSpec file that tests and waits for any necessary database changes before traffic can flow to the new version of the Lambda function
B. Add an AfterAllowTraffic hook to the AppSpec file that forces traffic to wait for any pending database changes before allowing the new version of the Lambda function to respond
C. Add a BeforeInstall hook to the AppSpec file that tests and waits for any necessary database changes before deploying the new version of the Lambda function
D. Add a ValidateService hook to the AppSpec file that inspects incoming traffic and rejects the payload if dependent services such as the database are not yet ready

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

**Explanation/Reference:**

**QUESTION 144**
A mobile application running on eight Amazon EC2 instances is relying on a third-party API endpoint. The third-party service has a high failure rate because of limited capacity, which is expected to be resolved in a few weeks.

In the meantime, the mobile application developers have added a retry mechanism and are logging failed API requests. A DevOps Engineer must automate the monitoring of application logs and count the specific error messages; if there are more than 10 errors within a 1-minute window, the system must issue an alert.

How can the requirements be met with MINIMAL management overhead?

A. Install the Amazon CloudWatch Logs agent on all instances to push the application logs to CloudWatch Logs. Use metric filters to count the error messages every minute, and trigger a CloudWatch alarm if the count exceeds 10 errors.
B. Install the Amazon CloudWatch Logs agent on all instances to push the access logs to CloudWatch Logs. Create a CloudWatch Events rule to count the error messages every minute, and trigger a CloudWatch alarm if the count exceeds 10 errors.
C. Install the Amazon CloudWatch Logs agent on all instances to push the application logs to CloudWatchLogs. Use a metric filter to generate a custom CloudWatch metric that records the number of failures and triggers a CloudWatch alarm if the custom metric reaches 10 errors in a 1-minute period.
D. Deploy a custom script on all instances to check application logs regularly in a cron job. Count the number of error messages every minute, and push a data point to a custom. CloudWatch metric. Trigger a CloudWatch alarm if the custom metric reaches 10 errors in a 1-minute period.

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

**Explanation/Reference:**

**QUESTION 145**
A DevOps Engineer has several legacy applications that all generate different log formats. The Engineer must standardize the formats before writing them to Amazon S3 for querying and analysis.

How can this requirement be met at the LOWEST cost?



A. Have the application send its logs to an Amazon EMR cluster and normalize the logs before sending them to Amazon S3
B. Have the application send its logs to Amazon QuickSight, then use the Amazon QuickSight SPICE engine to normalize the logs. Do the analysis directly from Amazon QuickSight
C. Keep the logs in Amazon S3 and use Amazon Redshift Spectrum to normalize the logs in place
D. Use Amazon Kinesis Agent on each server to upload the logs and have Amazon Kinesis Data Firehose use an AWS Lambda function to normalize the logs before writing them to Amazon S3

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

**Explanation/Reference:**

**QUESTION 146**
A company uses Amazon S3 to store proprietary information. The Development team creates buckets for new projects on a daily basis. The Security team wants to ensure that all existing and future buckets have encryption, logging, and versioning enabled. Additionally, no buckets should ever be publicly read or write

accessible.
What should a DevOps Engineer do to meet these requirements?

A. Enable AWS CloudTrail and configure automatic remediation using AWS Lambda.
B. Enable AWS Config rules and configure automatic remediation using AWS Systems Manager documents.
C. Enable AWS Trusted Advisor and configure automatic remediation using Amazon CloudWatch Events.
D. Enable AWS Systems Manager and configure automatic remediation using Systems Manager documents.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/aws/aws-config-update-new-managed-rules-to-secure-s3-buckets/

**QUESTION 147**
A DevOps Engineer is researching the least-expensive way to implement an image batch processing cluster in AWS. The application cannot run in Docker containers and must run on Amazon EC2. The batch job stores checkpoint data on a Network File System (NFS) and can tolerate interruptions. Configuring the cluster software from a bare EC2 Amazon Linux image takes 30 minutes.
Which is the MOST cost-effective solution?



A. Use Amazon EFS for checkpoint data. To complete the job, use an EC2 Auto Scaling group and an On-Demand pricing model to provision EC2 instances temporarily.
B. Use ClusterFS on EC2 instances for checkpoint data. To run the batch job, configure EC2 instances manually. When the job completes, shut down the instances manually.
C. Use Amazon EFS for checkpoint data. Use EC2 Fleet to launch EC2 Spot Instances, and use user data to configure the EC2 Amazon Linux instance on startup.
D. Use Amazon EFS for checkpoint data. Use EC2 Fleet to launch EC2 Spot Instances. Create a standard cluster AMI and use the latest AMI when creating instances.

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

**Explanation/Reference:**

**QUESTION 148**
A company is using AWS CodeDeploy to manage its application deployments. Recently, the Development team decided to use GitHub for version control, and

the team is looking for ways to integrate the GitHub repository with CodeDeploy. The team also needs to develop a way to automate deployment whenever there is a new commit on that repository. The team is currently deploying new application revisions by manually indicating the Amazon S3 location.
How can the integration be achieved in the MOST efficient way?

A. Create a GitHub webhook to replicate the repository to AWS CodeCommit. Create an AWS CodePipeline pipeline that uses CodeCommit as a source provider and AWS CodeDeploy as a deployment provider. Once configured, commit achange to the GitHub repository to start the first deployment.
B. Create an AWS CodePipeline pipeline that uses GitHub as a source provider and AWS CodeDeploy as a deployment provider. Connect this new pipeline with the GitHub account and instruct CodePipeline to use webhooks in GitHub toautomatically start the pipeline when a change occurs.
C. Create an AWS Lambda function to check periodically if there has been a new commit within the GitHub repository. If a new commit is found, trigger a CreateDeployment API call to AWS CodeDeploy to start a new deployment based onthe last commit ID within the deployment group.
D. Create an AWS CodeDeploy custom deployment configuration to associate the GitHub repository with the deployment group. During the association process, authenticate the deployment group with GitHub to obtain the GitHub securityauthentication token. Configure the deployment group options to automatically deploy if a new commit is found. Perform a new commit to the GitHub repository to trigger the first deployment.

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

**Explanation/Reference:**



**QUESTION 149**
A DevOps Engineer must implement monitoring for a workload running on Amazon EC2 and Amazon RDS MySQL. The monitoring must include:
Application logs and operating system metrics for the Amazon EC2 instances Database logs and operating system metrics for the Amazon RDS database
Which steps should the Engineer take?

A. Install an Amazon CloudWatch agent on the EC2 and RDS instances. Configure the agent to send the operating system metrics and application and database logs to CloudWatch.
B. Install an Amazon CloudWatch agent on the EC2 instance, and configure the agent to send the application logs and operating system metrics to CloudWatch. Enable RDS Enhanced Monitoring, and modify the RDS instance to publishdatabase logs to CloudWatch Logs.
C. Install an Amazon CloudWatch Logs agent on the EC2 instance and configure it to send application logs to CloudWatch.
D. Set up scheduled tasks on the EC2 and RDS instances to put operating system metrics and application and database logs into an Amazon S3 bucket. Set up an event on the bucket to invoke an AWS Lambda function to monitor forerrors each time an object is put into the bucket.

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

**Explanation/Reference:**

**QUESTION 150**
A company mandates the creation of capture logs for everything running in its AWS account. The account has multiple VPCs with Amazon EC2 instances, Application Load Balancers, Amazon RDS MySQL databases, and AWS WAF rules configured. The logs must be protected from deletion. A daily visual analysis of log anomalies from the previous day is required.
Which combination of actions should a DevOps Engineer take to accomplish this? (Choose three.)

A. Configure an AWS Lambda function to send all CloudWatch logs to an Amazon S3 bucket. Create a dashboard report in Amazon QuickSight.
B. Configure AWS CloudTrail to send all logs to Amazon Inspector. Create a dashboard report in Amazon QuickSight.
C. Configure Amazon S3 MFA Delete on the logging Amazon S3 bucket.
D. Configure an Amazon S3 object lock legal hold on the logging Amazon S3 bucket.
E. Configure AWS Artifact to send all logs to the logging Amazon S3 bucket. Create a dashboard report in Amazon QuickSight.
F. Deploy an Amazon CloudWatch agent to all Amazon EC2 instances.

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

**Explanation/Reference:**



**QUESTION 151**
A DevOps Engineer wants to prevent Developers from pushing updates directly to the company's master branch in AWS CodeCommit. These updates should be approved before they are merged.
Which solution will meet these requirements?

A. Configure an IAM role for the Developers with access to CodeCommit and an explicit deny for write actions when the reference is the master. Allow Developers to use feature branches and create a pull request when a feature iscomplete. Allow an approver to use CodeCommit to view the changes and approve the pull requests.
B. Configure an IAM role for the Developers to use feature branches and create a pull request when a feature is complete. Allow CodeCommit to test all code in the feature branches, and dynamically modify the IAM role to allow mergingthe feature branches into the master. Allow an approver to use CodeCommit to view the changes and approve the pull requests.
C. Configure an IAM role for the Developers to use feature branches and create a pull request when a feature is complete. Allow CodeCommit to test all code in the feature branches, and issue a new AWS Security Token Service (STS)token allowing a one-time API call to merge the feature branches into the master. Allow an approver to use CodeCommit to view the changes and approve the pull requests.
D. Configure an IAM role for the Developers with access to CodeCommit and attach an access policy to the CodeCommit repository that denies the Developers role access when the reference is master. Allow Developers to use featurebranches and create a pull request when a feature is complete. Allow an approver to use CodeCommit to view the changes and approve the pull requests.

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

**Explanation/Reference:**

**QUESTION 152**
A company is using AWS Organizations to create separate AWS accounts for each of its departments. It needs to automate the following tasks:

- Updating the Linux AMIs with new patches periodically and generating a golden image
- Installing a new version of Chef agents in the golden image, if available
- Enforcing the use of the newly generated golden AMIs in the department's account

Which option requires the LEAST management overhead?

A. Write a script to launch an Amazon EC2 instance from the previous golden AMI, apply the patch updates, install the new version of the Chef agent, generate a new golden AMI, and then modify the AMI permissions to share only the new image with the departments' accounts.
B. Use an AWS Systems Manager Run Command to update the Chef agent first, use Amazon EC2 Systems Manager Automation to generate an updated AMI, and then assume an IAM role to copy the new golden AMI into the departments' accounts.
C. Use AWS Systems Manager Automation to update the Linux AMI using the previous image, provide the URL for the script that will update the Chef agent, and then use AWS Organizations to replace the previous golden AMI into the departments' accounts.
D. Use AWS Systems Manager Automation to update the Linux AMI from the previous golden image, provide the URL for the script that will update the Chef agent, and then share only the newly generated AMI with the departments' accounts.

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

**Explanation/Reference:**

**QUESTION 153**
A company wants to automatically re-create its infrastructure using AWS CloudFormation as part of the company's quality assurance (QA) pipeline. For each QA run, a new VPC must be created in a single account, resources must be deployed into the VPC, and tests must be run against this new infrastructure. The company policy states that all VPCs must be peered with a central management VPC to allow centralized logging. The company has existing CloudFormation templates to deploy its VPC and associated resources.
Which combination of steps will achieve the goal in a way that is automated and repeatable? (Choose two.)

A. Create an AWS Lambda function that is invoked by an Amazon CloudWatch Events rule when a CreateVpcPeeringConnection API call is made. The Lambda function should check the source of the peering request, accepts the request,and update the route tables for the management VPC to allow traffic to go over the peering connection.

B. In the CloudFormation template:
Invoke a custom resource to generate unique VPC CIDR ranges for the VPC and subnets.
Create a peering connection to the management VPC.
Update route tables to allow traffic to the management VPC.

C. In the CloudFormation template:
Use the Fn::Cidr function to allocate an unused CIDR range for the VPC and subnets.
Create a peering connection to the management VPC.
Update route tables to allow traffic to the management VPC.

D. Modify the CloudFormation template to include a mappings object that includes a list of /16 CIDR ranges for each account where the stack will be deployed.

E. Use CloudFormation StackSets to deploy the VPC and associated resources to multiple AWS accounts using a custom resource to allocate unique CIDR ranges. Create peering connections from each VPC to the central managementVPC and accept those connections in the management VPC.

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

**Explanation/Reference:**



**QUESTION 154**
A company has multiple development groups working in a single shared AWS account. The Senior Manager of the groups wants to be alerted via a third-party API call when the creation of resources approaches the service limits for the account.
Which solution will accomplish this with the LEAST amount of development effort?

A. Create an Amazon CloudWatch Event rule that runs periodically and targets an AWS Lambda function. Within the Lambda function, evaluate the current state of the AWS environment and compare deployed resource values to resourcelimits on the account. Notify the Senior Manager if the account is approaching a service limit.

B. Deploy an AWS Lambda function that refreshes AWS Trusted Advisor checks, and configure an Amazon CloudWatch Events rule to run the Lambda function periodically. Create another CloudWatch Events rule with an event patternmatching Trusted Advisor events and a target Lambda function. In the target Lambda function, notify the Senior Manager.

C. Deploy an AWS Lambda function that refreshes AWS Personal Health Dashboard checks, and configure an Amazon CloudWatch Events rule to run the Lambda function periodically. Create another CloudWatch Events rule with anevent pattern matching Personal Health Dashboard events and a target Lambda function. In the target Lambda function, notify the Senior Manager.

D. Add an AWS Config custom rule that runs periodically, checks the AWS service limit status, and streams notifications to an Amazon SNS topic. Deploy an AWS Lambda function that notifies the Senior Manager, and subscribe theLambda function to the SNS topic.

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

**Explanation/Reference:**

**QUESTION 155**
A highly regulated company has a policy that DevOps Engineers should not log in to their Amazon EC2 instances except in emergencies. If a DevOps Engineer does log in, the Security team must be notified within 15 minutes of the occurrence.
Which solution will meet these requirements?

A. Install the Amazon Inspector agent on each EC2 instance. Subscribe to Amazon CloudWatch Events notifications. Trigger an AWS Lambda function to check if a message is about user logins. If it is, send a notification to the Securityteam using Amazon SNS.
B. Install the Amazon CloudWatch agent on each EC2 instance. Configure the agent to push all logs to Amazon CloudWatch Logs and set up a CloudWatch metric filter that searches for user logins. If a login is found, send a notification tothe Security team using Amazon SNS.
C. Set up AWS CloudTrail with Amazon CloudWatch Logs. Subscribe CloudWatch Logs to Amazon Kinesis. Attach AWS Lambda to Kinesis to parse and determine if a log contains a user login. If it does, send a notification to the Securityteam using Amazon SNS.
D. Set up a script on each Amazon EC2 instance to push all logs to Amazon S3. Set up an S3 event to trigger an AWS Lambda function, which triggers an Amazon Athena query to run. The Athena query checks for logins and sends theoutput to the Security team using Amazon SNS.



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

**Explanation/Reference:**

**QUESTION 156**
A DevOps Engineer manages a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group across multiple Availability Zones. The Engineer needs to implement a deployment strategy that:
Launches a second fleet of instances with the same capacity as the original fleet.
Maintains the original fleet unchanged while the second fleet is launched.
Transitions traffic to the second fleet when the second fleet is fully deployed. Terminates the original fleet automatically 1 hour after transition.
Which solution will satisfy these requirements?

A. Use an AWS CloudFormation template with a retention policy for the ALB set to 1 hour. Update the Amazon Route 53 record to reflect the new ALB.
B. Use two AWS Elastic Beanstalk environments to perform a blue/green deployment from the original environment to the new one. Create an application version lifecycle policy to terminate the original environment in 1 hour.
C. Use AWS CodeDeploy with a deployment group configured with a blue/green deployment configuration. Select the option Terminate the original instances in

the deployment group with a waiting period of 1 hour.

D. Use AWS Elastic Beanstalk with the configuration set to Immutable. Create an .ebextension using the Resources key that sets the deletion policy of the ALB to 1 hour, and deploy the application.

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

**Explanation/Reference:**

**QUESTION 157**
A company is using Docker containers for an application deployment and wants to move its application to AWS. The company currently manages its own clusters on premises to manage the deployment of these containers. It wants to deploy its application to a managed service in AWS and wants the entire flow of the deployment process to be automated. In addition, the company has the following requirements:
Focus first on the development workload.
The environment must be easy to manage.
Deployment should be repeatable and reusable for new environments. Store the code in a GitHub repository.
Which solution will meet these requirements?

A. Set up an Amazon ECS environment. Use AWS CodePipeline to create a pipeline that is triggered on a commit to the GitHub repository. Use AWS CodeBuild to create the container images and AWS CodeDeploy to publish the containerimage to the ECS environment.

B. Use AWS CodePipeline that triggers on a commit from the GitHub repository, build the container images with AWS CodeBuild, and publish the container images to Amazon ECR. In the final stage, use AWS CloudFormation to create anAmazon ECS environment that gets the container images from the ECR repository.

C. Create a Kubernetes Cluster on Amazon EC2. Use AWS CodePipeline to create a pipeline that is triggered when the code is committed to the repository. Create the container images with a Jenkins server on EC2 and store them in theDocker Hub. Use AWS Lambda from the pipeline to trigger the deployment to the Kubernetes Cluster.

D. Set up an Amazon ECS environment. Use AWS CodePipeline to create a pipeline that is triggered on a commit to the GitHub repository. Use AWS CodeBuild to create the container and store it in the Docker Hub. Use an AWS Lambdafunction to trigger a deployment and pull the new container image from the Docker Hub.

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

**Explanation/Reference:**

**QUESTION 158**

A company has migrated its container-based applications to Amazon EKS and wants to establish automated email notifications. The notifications sent to each email address are for specific activities related to EKS components. The solution will include Amazon SNS topics and an AWS Lambda function to evaluate incoming log events and publish messages to the correct SNS topic.
Which logging solution will support these requirements?

A. Enable Amazon CloudWatch Logs to log the EKS components. Create a CloudWatch subscription filter for each component with Lambda as the subscription feed destination.
B. Enable Amazon CloudWatch Logs to log the EKS components. Create CloudWatch Logs Insights queries linked to Amazon CloudWatch Events events that trigger Lambda.
C. Enable Amazon S3 logging for the EKS components. Configure an Amazon CloudWatch subscription filter for each component with Lambda as the subscription feed destination.
D. Enable Amazon S3 logging for the EKS components. Configure S3 PUT Object event notifications with AWS Lambda as the destination.

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

**Explanation/Reference:**



**QUESTION 159**
An n-tier application requires a table in an Amazon RDS MySQL DB instance to be dropped and repopulated at each deployment. This process can take several minutes and the web tier cannot come online until the process is complete. Currently, the web tier is configured in an Amazon EC2 Auto Scaling group, with instances being terminated and replaced at each deployment. The MySQL table is populated by running a SQL query through an AWS CodeBuild job.
What should be done to ensure that the web tier does not come online before the database is completely configured?

A. Use Amazon Aurora as a drop-in replacement for RDS MySQL. Use snapshots to populate the table with the correct data.
B. Modify the launch configuration of the Auto Scaling group to pause user data execution for 600 seconds, allowing the table to be populated.
C. Use AWS Step Functions to monitor and maintain the state of data population. Mark the database in service before continuing with the deployment.
D. Use an EC2 Auto Scaling lifecycle hook to pause the configuration of the web tier until the table is populated.

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

**Explanation/Reference:**

**QUESTION 160**

A web application with multiple services runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS Multi-AZ DB instance. The instance health check used by the load balancer returns PASS if at least one service is running on the instance.
The company uses AWS CodePipeline with AWS CodeBuild and AWS CodeDeploy steps to deploy code to test and production environments. Recently, a new version was unable to connect to the database server in the test environment. One process was running, so the health checks reported healthy and the application was promoted to production, causing a production outage. The company wants to ensure that test builds are fully functional before a promotion to production.
Which changes should a DevOps Engineer make to the test and deployment process? (Choose two.)

A. Add an automated functional test to the pipeline that ensures solid test cases are performed.
B. Add a manual approval action to the CodeDeploy deployment pipeline that requires a Testing Engineer to validate the testing environment.
C. Refactor the health check endpoint the Elastic Load Balancer is checking to better validate actual application functionality.
D. Refactor the health check endpoint the Elastic Load Balancer is checking to return a text-based status result and configure the load balancer to check for a valid response.
E. Add a dependency checking step to the existing testing framework to ensure compatibility.

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

**Explanation/Reference:**



**QUESTION 161**
A company's application is currently deployed to a single AWS Region. Recently, the company opened a new office on a different continent. The users in the new office are experiencing high latency. The company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) and uses Amazon DynamoDB as the database layer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. A DevOps Engineer is tasked with minimizing application response times and improving availability for users in both Regions.
Which combination of actions should be taken to address the latency issues? (Choose three.)

A. Create a new DynamoDB table in the new Region with cross-Region replication enabled.
B. Create new ALB and Auto Scaling group global resources and configure the new ALB to direct traffic to the new Auto Scaling group.
C. Create new ALB and Auto Scaling group resources in the new Region and configure the new ALB to direct traffic to the new Auto Scaling group.
D. Create Amazon Route 53 records, health checks, and latency-based routing policies to route to the ALB.
E. Create Amazon Route 53 aliases, health checks, and failover routing policies to route to the ALB.
F. Convert the DynamoDB table to a global table.

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

**Explanation/Reference:**

**QUESTION 162**
A security review has identified that an AWS CodeBuild project is downloading a database population script from an Amazon S3 bucket using an unauthenticated request. The Security team does not allow unauthenticated requests to S3 buckets for this project.
How can this issue be corrected in the MOST secure manner?

A. Add the bucket name to the AllowedBuckets section of the CodeBuild project settings. Update the build spec to use the AWS CLI to download the database population script.
B. Modify the S3 bucket settings to enable HTTPS basic authentication and specify a token. Update the build spec to use cURL to pass the token and download the database population script.
C. Remove unauthenticated access from the S3 bucket with a bucket policy. Modify the service role for the CodeBuild project to include Amazon S3 access. Use the AWS CLI to download the database population script.
D. Remove unauthenticated access from the S3 bucket with a bucket policy. Use the AWS CLI to download the database population script using an IAM access key and a secret access key.

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



**Explanation/Reference:**

**QUESTION 163**
A DevOps Engineer is deploying an Amazon API Gateway API with an AWS Lambda function providing the backend functionality. The Engineer needs to record the source IP address and response status of every API call. Which combination of actions should the DevOps Engineer take to implement this functionality? (Choose three.)

A. Configure AWS X-Ray to enable access logging for the API Gateway requests.
B. Configure the API Gateway stage to enable access logging and choose a logging format.
C. Create a new Amazon CloudWatch Logs log group or choose an existing log group to store the logs.
D. Grant API Gateway permission to read and write logs to Amazon CloudWatch through an IAM role.
E. Create a new Amazon S3 bucket or choose an existing S3 bucket to store the logs.
F. Configure API Gateway to stream its log data to Amazon Kinesis.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 164**
A DevOps Engineer at a startup cloud-based gaming company has the task of formalizing deployment strategies. The strategies must meet the following requirements:
Use standard Git commands, such as `git clone` and `git push` for the code repository. Management tools should maximize the use of platform solutions where possible.
Deployment packages must be immutable and in the form of Docker images.
How can the Engineer meet these requirements?

A. Use AWS CodePipeline to trigger a build process when software is pushed to a self-hosted GitHub repository. CodePipeline will use a Jenkins build server to build new Docker images. CodePipeline will deploy into a second target groupin Amazon ECS behind an Application Load Balancer. Cutover will be managed by swapping the listener rules on the Application Load Balancer.
B. Use AWS CodePipeline to trigger a build process when software is pushed to a private GitHub repository. CodePipeline will use AWS CodeBuild to build new Docker images. CodePipeline will deploy into a second target group inAmazon ECS behind an Application Load Balancer. Cutover will be managed by swapping the listener rules on the Application Load Balancer.
C. Use a Jenkins pipeline to trigger a build process when software is pushed to a private GitHub repository. AWS CodePipeline will use AWS CodeBuild to build new Docker images. CodePipeline will deploy into a second target group in AmazonECS behind an Application Load Balancer. Cutover will be managed by swapping the listener rules on the Application Load Balancer.
D. Use AWS CodePipeline to trigger a build process when software is pushed to an AWS CodeCommit repository CodePipeline will use an AWS CodeBuild build server to build new Docker images. CodePipeline will deploy into a secondtarget group in a Kubernetes Cluster hosted on Amazon EC2 behind an Application Load Balancer. Cutover will be managed by swapping the listener rules on the Application Load Balancer.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/devops/build-a-continuous-delivery-pipeline-for-your-container-images-with-amazon-ecr-as-source/

**QUESTION 165**
An application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). A DevOps Engineer is using AWS CodeDeploy to release a new version. The deployment fails during the AllowTraffic lifecycle event, but a cause for the failure is not indicated in the deployment logs.
What would cause this?

A. The appspec.yml file contains an invalid script to execute in the AllowTraffic lifecycle hook.
B. The user who initiated the deployment does not have the necessary permissions to interact with the ALB.

C. The health checks specified for the ALB target group are misconfigured.
D. The CodeDeploy agent was not installed in the EC2 instances that are part of the ALB target group.

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

**Explanation/Reference:**
Reference: https://docs.amazonaws.cn/en_us/codedeploy/latest/userguide/codedeploy-user.pdf (399)

**QUESTION 166**
A company is deploying a container-based application using AWS CodeBuild. The Security team mandates that all containers are scanned for vulnerabilities prior to deployment using a password-protected endpoint. All sensitive information must be stored securely.
Which solution should be used to meet these requirements?

A. Encrypt the password using AWS KMS. Store the encrypted password in the buildspec.yml file as an environment variable under the variables mapping. Reference the environment variable to initiate scanning.
B. Import the password into an AWS CloudHSM key. Reference the CloudHSM key in the buildpec.yml file as an environment variable under the variables mapping. Reference the environment variable to initiate scanning.
C. Store the password in the AWS Systems Manager Parameter Store as a secure string. Add the Parameter Store key to the buildspec.yml file as an environment variable under the parameter-store mapping. Reference the environmentvariable to initiate scanning.
D. Use the AWS Encryption SDK to encrypt the password and embed in the buildspec.yml file as a variable under the secrets mapping. Attach a policy to CodeBuild to enable access to the required decryption key.

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

**Explanation/Reference:**

**QUESTION 167**
A DevOps Engineer must ensure all IAM entity configurations across multiple AWS accounts in AWS Organizations are compliant with corporate IAM policies.
Which combination of steps will accomplish this? (Choose two.)

A. Enable AWS Trusted Advisor in Organizations for all accounts to report on noncompliant IAM entities.
B. Configure an AWS Config aggregator in the Organizations master account for all accounts.
C. Deploy AWS Config rules to the master account in Organizations that match corporate IAM policies.
D. Apply an SCP in Organizations to ensure compliance of IAM entities.

E. Deploy AWS Config rules to all accounts in Organizations that match the corporate IAM policies.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/mt/manage-custom-aws-config-rules-with-remediations-using-conformance-packs/?nc1=b_rp https://aws.amazon.com/blogs/security/announcing-aws-organizations-centrally-manage-multiple-aws-accounts/

**QUESTION 168**
A company has thousands of Amazon EC2 instances as well as hundreds of virtual machines on-premises. Developers routinely sign in to the console for on-premises systems to perform troubleshooting. The Developers want to sign in to AWS instances to run performance tools, but are unable to due to the lack of a central console logging system. A DevOps Engineer wants to ensure that console access is logged on all systems.
Which combination of steps will meet these requirements? (Choose two.)

A. Attach a role to all AWS instances that contains the appropriate permissions. Create an AWS Systems Manager managed-instance activation. Install and configure Systems Manager Agent on on-premises machines.
B. Enable AWS Systems Manager Session Manager logging to an Amazon S3 bucket. Direct Developers to connect to the systems with Session Manager only.
C. Enable AWS Systems Manager Session Manager logging to AWS CloudTrail. Direct Developers to continue normal sign-in procedures for on-premises. Use Session Manager for AWS instances.
D. Install and configure an Amazon CloudWatch Logs agent on all systems. Create an AWS Systems Manager managed-instance activation.
E. Set up a Site-to-Site VPN connection between the on-premises and AWS networks. Set up a bastion instance to allow Developers to sign in to the AWS instances.

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

**Explanation/Reference:**

**QUESTION 169**
A DevOps team wants to be able to work on the same source code repository. The team has the following requirements for their development workflow and repository access controls:
Only team members can clone the repository and create new branches.
A production-ready code state should be isolated from any untested code changes.
Code changes should be approved by another team member before merging to the production-ready master branch. All code change approvals must have an audit record. New team members can quickly modify code.
Which combination of actions will these requirements? (Choose three.)

A. Check out the master branch and develop new features locally on a feature branch to keep the production-ready code isolated. Ask team members to review the changes before committing the changes locally.
B. Create an AWS CodeCommit repository and an IAM group with permissions to read/write changes to the repository. Add new team members to this group.
C. Create an AWS CodeCommit repository and an IAM role with permissions to read/write changes to the repository. Attach this IAM role to a single IAM user. Ensure each member of the team uses this IAM user. Provide new teammembers the credentials to this IAM user.
D. Create a local feature branch from the master branch for new features. Commit the new code and push the changes to the feature branch in the repository.
E. Create a pull request so other team members can review the code changes. Implement any suggestions, pull any additional changes from the master branch, and push to the feature branch again. Merge the master branch with thefeature branch.
F. Create a pull request so other team members can review the code changes. Implement any suggestions, pull any additional changes from the master branch, resolve any conflicts, and push to the feature branch again. Merge the featurebranch with the master branch.

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

**Explanation/Reference:**

**QUESTION 170**
A company has a web application that uses an Amazon DynamoDB table in a single AWS Region to store user information. To support an increasingly global user base, the application must run in a secondary Region and allow users to connect to their closest Region and fail over to the secondary Region.
Which approach should be used to ensure the deployment meets these requirements?

A. Configure DynamoDB streams to copy data between Regions, deploy the web stack in both Regions, and configure Amazon Route 53 to use a geoproximity routing policy with health checks.
B. Convert the DynamoDB table to a global table, deploy the web stack in both Regions, and configure Amazon Route 53 to use a geoproximity routing policy with health checks.
C. Define DynamoDB cross-region backups to copy data to the secondary Region, deploy the web stack in both Regions, and configure Amazon Route 53 to use a latency-based routing policy with health checks.
D. Use DynamoDB Accelerator to copy data to the secondary Region, deploy the web stack in both Regions, and configure Amazon Route 53 to use a failover routing policy.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/database/how-to-use-amazon-dynamodb-global-tables-to-power-multiregion-architectures/

**QUESTION 171**
An ecommerce company uses a large number of Amazon EBS backed Amazon EC2 instances. To decrease manual work across all the instances, a DevOps Engineer is tasked with automating restart actions when EC2 instance retirement events are scheduled.
How can this be accomplished?

A. Create a scheduled Amazon CloudWatch Events rule to execute an AWS Systems Manager automation document that checks if any EC2 instances are scheduled for retirement once a week. If the instance is scheduled for retirement,the automation document will hibernate the instance.
B. Enable EC2 Auto Recovery on all of the instances. Create an AWS Config rule to limit the recovery to occur during a maintenance window only.
C. Reboot all EC2 instances during an approved maintenance window that is outside of standard business hours. Set up Amazon CloudWatch alarms to send a notification in case any instance is failing EC2 instance status checks.
D. Set up an AWS Health Amazon CloudWatch Events rule to execute AWS Systems Manager automation documents that stop and start the EC2 instance when a retirement scheduled event occurs.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/mt/automate-remediation-actions-for-amazon-ec2-notifications-and-beyond-using-ec2-systems-manager-automation-and-aws-health/



**QUESTION 172**
A company has containerized all of its in-house quality control applications. The company is running Jenkins on Amazon EC2, which requires patching and upgrading. The Compliance Officer has requested a DevOps Engineer begin encrypting build artifacts since they contain company intellectual property.
What should the DevOps Engineer do to accomplish this in the MOST maintainable manner?

A. Automate patching and upgrading using AWS Systems Manager on EC2 instances and encrypt Amazon EBS volumes by default.
B. Deploy Jenkins to an Amazon ECS cluster and copy build artifacts to an Amazon S3 bucket with default encryption enabled.
C. Leverage AWS CodePipeline with a build action and encrypt the artifacts using AWS Secrets Manager.
D. Use AWS CodeBuild with artifact encryption to replace the Jenkins instance running on Amazon EC2.

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

**Explanation/Reference:**

**QUESTION 173**
A DevOps Engineer is setting up a container-based architecture. The Engineer has decided to use AWS CloudFormation to automatically provision an Amazon ECS cluster and an Amazon EC2 Auto Scaling group to launch the EC2 container instances. After successfully creating the CloudFormation stack, the Engineer noticed that, even though the ECS cluster and the EC2 instances were created successfully and the stack finished the creation, the EC2 instances were associating with a different cluster.
How should the DevOps Engineer update the CloudFormation template to resolve this issue?

A. Reference the EC2 instances in the AWS::ECS::Cluster resource and reference the ECS cluster in the AWS::ECS::Service resource.
B. Reference the ECS cluster in the AWS::AutoScaling::LaunchConfiguration resource of the UserData property.
C. Reference the ECS cluster in the AWS::EC2::Instance resource of the UserData property.
D. Reference the ECS cluster in the AWS::CloudFormation::CustomResource resource to trigger an AWS Lambda function that registers the EC2 instances with the appropriate ECS cluster.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as-launchconfig.html

**QUESTION 174**
A company indexes all of its Amazon CloudWatch Logs on Amazon ES and uses Kibana to view a dashboard for actionable insight. The company wants to restrict user access to Kibana by user.
Which actions can a DevOps Engineer take to meet this requirement? (Choose two.)

A. Create a proxy server with user authentication in an Auto Scaling group, and restrict access of the Amazon ES endpoint to an Auto Scaling group tag.
B. Create a proxy server with user authentication and an Elastic IP address, and restrict access of the Amazon ES endpoint to the IP address.
C. Create a proxy server with AWS IAM user, and restrict access of the Amazon ES endpoint to the IAM user.
D. Use AWS SSO to offer user name and password protection for Kibana.
E. Use Amazon Cognito to offer user name and password protection for Kibana.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-cognito-auth.html

**QUESTION 175**

A company's DevOps team launches a WorkSpace using Amazon WorkSpaces for each new user. Recently, the Security team said that WorkSpaces for these new users are not consistently being tagged. Company policy requires that all WorkSpaces be tagged with USERNAME automatically upon creation.
Which combination of steps should the DevOps Engineer take to address this requirement? (Choose two.)

A. Add an AWS Lambda function policy allowing cloudtrail.amazonaws.com to use the lambda:InvokeFunction action.
B. Create a new Amazon CloudWatch Events event pattern rule based on Amazon WorkSpaces with an AWS API Call via CloudTrail event type. Select the CreateWorkspaces operation, and target an AWS Lambda function that will tagthe Workspace.
C. Ensure AWS CloudTrail is enabled in all Regions where WorkSpaces are created.
D. Enable custom tagging for Amazon WorkSpaces from the directory details.
E. Create a new Amazon CloudWatch Events scheduled event rule based on Amazon WorkSpaces with an interval of 1 minute. Target an AWS Lambda function that will tag the Workspace.

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

**Explanation/Reference:**



**QUESTION 176**
A company has a mission-critical application on AWS that uses automatic scaling. The company wants the deployment lifecycle to meet the following parameters:
- The application must be deployed one instance at a time to ensure the remaining fleet continues to serve traffic.
- The application is CPU intensive and must be closely monitored.
- The deployment must automatically roll back if the CPU utilization of the deployment instance exceeds 85%.
Which solution will meet these requirements?

A. Use AWS CloudFormation to create an AWS Step Functions state machine and Auto Scaling lifecycle hooks to move to one instance at a time into a wait state. Use AWS Systems Manager automation to deploy the update to eachinstance and move it back into the Auto Scaling group using the heartbeat timeout.
B. Use AWS CodeDeploy with Amazon EC2 Auto Scaling. Configure an alarm tied to the CPU utilization metric. Use the CodeDeployDefault.OneAtAtime configuration as a deployment strategy. Configure automatic rollbacks within thedeployment group to roll back the deployment if the alarm thresholds are breached.
C. Use AWS Elastic Beanstalk for load balancing and AWS Auto Scaling. Configure an alarm tied to the CPU utilization metric. Configure rolling deployments with a fixed batch size of one instance. Enable enhanced health to monitor thestatus of the deployment and roll back based on the alarm previously created.
D. Use AWS Systems Manager to perform a blue/green deployment with Amazon EC2 Auto Scaling. Configure an alarm tied to the CPU utilization metric. Deploy updates one at a time. Configure automatic rollbacks within the Auto Scalinggroup to roll back the deployment if the alarm thresholds are breached.

**Correct Answer:** B

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/about-aws/whats-new/2016/09/aws-codedeploy-introduces-deployment-monitoring-with-amazon-cloudwatch-alarms-and-automatic-deployment-rollback/

**QUESTION 177**
A DevOps Engineer is architecting a continuous development strategy for a company's software as a service (SaaS) web application running on AWS. For application and security reasons, users subscribing to this application are distributed across multiple Application Load Balancers (ALBs), each of which has a dedicated Auto Scaling group and fleet of Amazon EC2 instances. The application does not require a build stage, and when it is committed to AWS CodeCommit, the application must trigger a simultaneous deployment to all ALBs, Auto Scaling groups, and EC2 fleets.
Which architecture will meet these requirements with the LEAST amount of configuration?

A. Create a single AWS CodePipeline pipeline that deploys the application in parallel using unique AWS CodeDeploy applications and deployment groups created for each ALB-Auto Scaling group pair.
B. Create a single AWS CodePipeline pipeline that deploys the application using a single AWS CodeDeploy application and single deployment group.
C. Create a single AWS CodePipeline pipeline that deploys the application in parallel using a single AWS CodeDeploy application and unique deployment group for each ALB-Auto Scaling group pair.
D. Create an AWS CodePipeline pipeline for each ALB-Auto Scaling group pair that deploys the application using an AWS CodeDeploy application and deployment group created for the same ALB-Auto Scaling group pair.



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

**Explanation/Reference:**

**QUESTION 178**
A DevOps Engineer needs to back up sensitive Amazon S3 objects that are stored within an S3 bucket with a private bucket policy using the S3 cross-region replication functionality. The objects need to be copied to a target bucket in a different AWS Region and account.
Which actions should be performed to enable this replication? (Choose three.)

A. Create a replication IAM role in the source account.
B. Create a replication IAM role in the target account.
C. Add statements to the source bucket policy allowing the replication IAM role to replicate objects.
D. Add statements to the target bucket policy allowing the replication IAM role to replicate objects.
E. Set AccessControlTranslation.OwnerOverride to true in the replication configuration and add a statement to the target bucket policy allowing the replication

IAM role to override object ownership.

F. Set AccessControlTranslation.Owner to destination in the replication configuration and add a statement to the target bucket policy allowing the replication IAM role to override object ownership.

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

**Explanation/Reference:**

**QUESTION 179**
A company is running an application on Amazon EC2 instances in an Auto Scaling group. Recently, an issue occurred that prevented EC2 instances from launching successfully, and it took several hours for the Support team to discover the issue. The Support team wants to be notified by email whenever an EC2 instance does not start successfully.
Which action will accomplish this?

A. Add a health check to the Auto Scaling group to invoke an AWS Lambda function whenever an instance status is impaired.
B. Configure the Auto Scaling group to send a notification to an Amazon SNS topic whenever a failed instance launch occurs.
C. Create an Amazon CloudWatch alarm that invokes an AWS Lambda function when a failed AttachInstances Auto Scaling API call is made.
D. Create a status check alarm on Amazon EC2 to send a notification to an Amazon SNS topic whenever a status check fail occurs.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/ec2-email-instance-state-change/

**QUESTION 180**
A company runs an application with an Amazon EC2 and on-premises configuration. A DevOps Engineer needs to standardize patching across both environments. Company policy dictates that patching only happens during non-business hours.
Which combination of actions will meet these requirements? (Choose three.)

A. Add the physical machines into AWS Systems Manager using Systems Manager Hybrid Activations.
B. Attach an IAM role to the EC2 instances, allowing them to be managed by AWS Systems Manager.
C. Create IAM access keys for the on-premises machines to interact with AWS Systems Manager.
D. Execute an AWS Systems Manager Automation document to patch the systems every hour.
E. Use Amazon CloudWatch Events scheduled events to schedule a patch window.

F. Use AWS Systems Manager Maintenance Windows to schedule a patch window.

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

**Explanation/Reference:**

**QUESTION 181**
A company's popular global web application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB) using an Auto Scaling group. The company is launching a new feature and expects unpredictable spikes in web traffic. The site currently includes a large amount of media content, and the new feature adds the ability to submit ratings and comments that will be stored in a new Amazon DynamoDB table. A DevOps Engineer is tasked with ensuring the web application can scale with the increased traffic and workload
Which combination of steps will accomplish this? (Choose two.)

A. Configure an Amazon CloudFront distribution to cache the web application's static and dynamic content.
B. Configure the web application's ALB to cache content in Amazon ElastiCache, honoring the HTTP cache headers.
C. Process the new ratings and comments asynchronously using Amazon SQS.
D. Replace the DynamoDB table with DynamoDB Accelerator to store the ratings and comments to reduce latency.
E. Set up AWS Global Accelerator to cache static content and pass dynamic requests to the web application's ALB endpoint.

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

**Explanation/Reference:**

**QUESTION 182**
An application is deployed on Amazon EC2 instances running in an Auto Scaling group. During the bootstrapping process, the instances register their private IP addresses with a monitoring system. The monitoring system performs health checks frequently by sending ping requests to those IP addresses and sending alerts if an instance becomes non-responsive.

The existing deployment strategy replaces the current EC2 instances with new ones. A DevOps Engineer has noticed that the monitoring system is sending false alarms during a deployment, and is tasked with stopping these false alarms.

Which solution will meet these requirements without affecting the current deployment method?

A. Define an Amazon CloudWatch Events target, an AWS Lambda function, and a lifecycle hook attached to the Auto Scaling group. Configure CloudWatch

Events to invoke Amazon SNS to send a message to the Systems Administrator group for remediation.

B. Define an AWS Lambda function and a lifecycle hook attached to the Auto Scaling group. Configure the lifecycle hook to invoke the Lambda function, which removes the entry of the private IP from the monitoring system upon instance termination.

C. Define an Amazon CloudWatch Events target, and AWS Lambda function, and a lifecycle hook attached to the Auto Scaling group. Configure CloudWatch Events to invoke the Lambda function, which removes the entry of the private IP from the monitoring system upon instance termination.

D. Define an AWS Lambda function that will run a script when instance termination occurs in an Auto Scaling group. The script will remove the entry of the private IP from the monitoring system.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/compute/using-aws-lambda-with-auto-scaling-lifecycle-hooks/

**QUESTION 183**
An application that runs on Amazon EC2 instances behind an Application Load Balancer is deployed using AWS Elastic Beanstalk. During a recent rolling deployment, users experienced application errors even though application health checks were passing on all instances. A log analysis shows that the errors were caused by user requests being processed by two different versions of the application behind the same load balancer. The analysis also shows a recent change made the responses backward incompatible.



Which deployment method will address these issues?

A. Update Elastic Beanstalk to deploy using the all at once method.

B. Update Elastic Beanstalk to deploy using the blue/green method.

C. Update Elastic Beanstalk to deploy using the immutable method.

D. Update Elastic Beanstalk to deploy using the rolling with additional batch method.

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

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

**QUESTION 184**
A DevOps Engineer is tasked with moving a mission-critical business application running in Go to AWS. The Development team running this application is understaffed and requires a solution that allows the team to focus on application development. They also want to enable blue/green deployments and perform A/B testing.

Which solution will meet these requirements?

A. Deploy the application on an Amazon EC2 instance and create an AMI of this instance. Use this AMI to create an automatic scaling launch configuration that is used in an Auto Scaling group. Use an Elastic Load Balancer to distribute traffic. When changes are made to the application, a new AMI is created and replaces the launch configuration.
B. Use Amazon Lightsail to deploy the application. Store the application in a zipped format in an Amazon S3 bucket. Use this zipped version to deploy new versions of the application to Lightsail. Use Lightsail deployment options to manage the deployment.
C. Use AWS CodePipeline with AWS CodeDeploy to deploy the application to a fleet of Amazon EC2 instances. Use an Elastic Load Balancer to distribute the traffic to the EC2 instances. When making changes to the application, upload a new version to CodePipeline and let it deploy the new version.
D. Use AWS Elastic Beanstalk to host the application. Store a zipped version of the application in Amazon S3, and use that location to deploy new versions of the application using Elastic Beanstalk to manage the deployment options.

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

**Explanation/Reference:**



**QUESTION 185**
An ecommerce company is looking for ways to deploy an application on AWS that satisfies the following requirements:

- Has a simple and automated application deployment process.
- Has minimal deployment costs while ensuring that at least half of the instances are available to receive end-user requests.
- If the application fails, an automated healing mechanism will replace the affected instances.

Which deployment strategy will meet these requirements?

A. Create an AWS Elastic Beanstalk environment and configure it to use Auto Scaling and an Elastic Load Balancer. Use rolling deployments with a batch size of 50%.
B. Create an AWS OpsWorks stack. Configure the application layer to use rolling deployments as a deployment strategy. Add an Elastic Load Balancing layer. Enable auto healing on the application layer.
C. Use AWS CodeDeploy with Auto Scaling and an Elastic Load Balancer. Use the CodeDeployDefault. HalfAtAtime deployment strategy. Enable an Elastic Load Balancing health check to report the status of the application, and set the Auto Scaling health check to ELB.
D. Use AWS CodeDeploy with Auto Scaling and an Elastic Load Balancer. Use a blue/green deployment strategy. Enable an Elastic Load Balancing health check to report the status of the application, and set the Auto Scaling health check to ELB.

**Correct Answer:** D

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

**Explanation/Reference:**

**QUESTION 186**
A DevOps engineer is tasked with migrating Docker containers used for a workload to AWS. The solution must allow for changes to be deployed into development and test environments automatically by updating each container and checking it into a container registry. Once the containers are pushed, they must be deployed automatically.

Which solution will meet these requirements?

A. Store container images in Amazon S3. Run the containers in AWS Elastic Beanstalk using a multicontainer Docker environment. Configure Elastic Beanstalk to redeploy the containers if it detects a new version in Amazon S3.
B. Store container images in AWS Artifact. Use AWS CodePipeline to trigger a deployment if a new container version is created. Use AWS CodeDeploy to deploy new containers to Amazon EKS.
C. Store container images in Amazon ECR. Use AWS CodePipeline to trigger a deployment if a new container version is created. Use AWS CodeDeploy to deploy the image to AWS Fargate.
D. Store container images in Docker Hub. Install Docker on an Amazon EC2 instance and use AWS CodePipeline and AWS CodeDeploy to deploy any new containers.



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

**Explanation/Reference:**

**QUESTION 187**
A Development team wants to deploy an application using AWS CloudFormation stacks, but the Developer IAM role does not currently have the required permissions to provision the resources specified in the CloudFormation template. A DevOps Engineer is tasked with allowing Developers to deploy the stacks while following the principal of least privilege.

Which solution will meet these requirements?

A. Create an IAM policy that allows Developers to provision the required resources. Attach the policy to the Developer role.
B. Create an IAM policy that allows full access to CloudFormation. Attach the policy to the Developer role.
C. Create a new IAM role with the required permissions to use as a CloudFormation service role. Grant the Developer role a cloudformation:* action.

D. Create a new IAM role with the required permissions to use as a CloudFormation service role. Grant the Developer role the iam:PassRole permission.

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

**Explanation/Reference:**

**QUESTION 188**
A company plans to stop using Amazon EC2 key pairs for SSH access, and instead plans to use AWS Systems Manager Session Manager. To further enhance security, access to Session Manager must take place over a private network only.

Which combinations of actions will accomplish this? (Choose two.)

A. Allow inbound access to TCP port 22 in all associated EC2 security groups from the VPC CIDR range.
B. Attach an IAM policy with the necessary Systems Manager permissions to the existing IAM instance profile.
C. Create a VPC endpoint for Systems Manager in the desired Region.
D. Deploy a new EC2 instance that will act as a bastion host to the rest of the EC2 instance fleet.
E. Remove any default routes in the associated route tables.



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

**Explanation/Reference:**

**QUESTION 189**
A company recently launched an application that is more popular than expected. The company wants to ensure the application can scale to meet increasing demands and provide reliability using multiple Availability Zones (AZs). The application runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). A DevOps engineer has created an Auto Scaling group across multiple AZs for the application. Instances launched in the newly added AZs are not receiving any traffic for the application.
What is likely causing this issue?

A. Auto Scaling groups can create new instances in a single AZ only.
B. The EC2 instances have not been manually associated to the ALB.
C. The ALB should be replaced with a Network Load Balancer (NLB).
D. The new AZ has not been added to the ALB.

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

**Explanation/Reference:**

**QUESTION 190**
A DevOps engineer has automated a web service deployment using AWS CodePipeline with the following steps:

- An AWS CodeBuild project compiles the deployment artifact and runs unit tests.
- An AWS CodeDeploy deployment group deploys the web service to Amazon EC2 instances in the staging environment.
- A CodeDeploy deployment group deploys the web service to EC2 instances in the production environment.

The quality assurance (QA) team has asked for permission to inspect the build artifact before the deployment to the production environment occurs. The QA team wants to run an internal automated penetration testing tool (invoked using a REST API call) to run some manual tests.

Which combination of actions will fulfill this request? (Choose two.)

A. Insert a manual approval action between the test and deployment actions of the pipeline.
B. Modify the buildspec.yml file for the compilation stage to require manual approval before completion.
C. Update the CodeDeploy deployment group so it requires manual approval to proceed.
D. Update the pipeline to directly trigger the REST API for the automated penetration testing tool.
E. Update the pipeline to invoke a Lambda function that triggers the REST API for the automated penetration testing tool.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/codebuild/latest/userguide/sample-codedeploy.html

**QUESTION 191**
A development team manually builds an artifact locally and then places it in an Amazon S3 bucket. The application has a local cache that must be cleared when a deployment occurs. The team executes a command to do this, downloads the artifact from Amazon S3, and unzips the artifact to complete the deployment.
A DevOps team wants to migrate to a CI/CD process and build in checks to stop and roll back the deployment when a failure occurs. This requires the team to track the progression of the deployment.
Which combination of actions will accomplish this? (Choose three.)

A. Allow developers to check the code into a code repository. Using Amazon CloudWatch Events, on every pull into master, trigger an AWS Lambda function to build the artifact and store it in Amazon S3.
B. Create a custom script to clear the cache. Specify the script in the BeforeInstall lifecycle hook in the AppSpec file.
C. Create user data for each Amazon EC2 instance that contains the clear cache script. Once deployed, test the application. If it is not successful, deploy it again.
D. Set up AWS CodePipeline to deploy the application. Allow developers to check the code into a code repository as a source for the pipeline.
E. Use AWS CodeBuild to build the artifact and place it in Amazon S3. Use AWS CodeDeploy to deploy the artifact to Amazon EC2 instances.
F. Use AWS Systems Manager to fetch the artifact from Amazon S3 and deploy it to all the instances.

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

**Explanation/Reference:**

**QUESTION 192**
A law firm is running a web application on AWS. The system manages legal documents uploaded by users, and stores the documents in Amazon S3. Users have complained that file uploads are taking too long and there are timeouts during peak usage. A DevOps engineer found that web servers are managing concurrent uploads and are overloaded.
Which actions should be taken to troubleshoot the issue in the MOST cost-effective manner?



A. Create an AWS CloudFront distribution in front of the web servers, and modify the application to upload to Amazon S3 using S3 Transfer Acceleration.
B. Modify the application so the browser uses a signed URL to directly upload to Amazon S3 using multipart uploads.
C. Create an AWS CloudFront distribution in front of the web servers, and modify the application to store files in Amazon EFS in the Max I/O performance mode.
D. Place the web servers in an Amazon EC2 Auto Scaling group to include Spot Instances and modify the application to upload to Amazon S3 using multipart uploads.

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

**Explanation/Reference:**
Section: (none)

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/s3-troubleshoot-slow-downloads-uploads/

**QUESTION 193**

An ecommerce company is running an application on AWS. The company wants to create a standby disaster recovery solution in an additional Region that keeps the current application code. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group across multiple Availability Zones. The database layer is hosted on an Amazon RDS MySQL Multi-AZ DB instance. Amazon Route 53 DNS records point to the ALB.
Which combination of actions will meet these requirements with the LOWEST cost? (Choose three.)

A. Configure a failover routing policy for the application DNS entry.
B. Configure a geolocation routing policy for the application DNS entry.
C. Create a cross-Region RDS read replica in the new standby Region.
D. Migrate the database layer to Amazon DynamoDB and enable global replication to the new standby Region.
E. Provision the ALB and Auto Scaling group in the new standby Region and set the desired capacity to match the active Region.
F. Provision the ALB and Auto Scaling group in the new standby Region and set the desired capacity to 1.

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

**Explanation/Reference:**



**QUESTION 194**
A DevOps engineer is creating a CI/CD pipeline for an Amazon ECS service. The ECS container instances run behind an Application Load Balancer as the web tier of a three-tier application. An acceptance criterion for a successful deployment is the verification that the web tier can communicate with the database and middleware tiers of the application upon deployment.
How can this be accomplished in an automated fashion?

A. Create a health check endpoint in the web application that tests connectivity to the data and middleware tiers. Use this endpoint as the health check URL for the load balancer.
B. Create an approval step for the quality assurance team to validate connectivity. Reject changes in the pipeline if there is an issue with connecting to the dependent tiers.
C. Use an Amazon RDS active connection count and an Amazon CloudWatch ELB metric to alarm on a significant change to the number of open connections.
D. Use Amazon Route 53 health checks to detect issues with the web service and roll back the CI/CD pipeline if there is an error.

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

**Explanation/Reference:**

**QUESTION 195**
A DevOps team wants to implement their containerized application using AWS. The deployment must meet the following requirements:
There should be minimal downtime during deployment.
The application must be functionally tested to be considered a success.
How can the DevOps team automate this deployment?

A. Use AWS Elastic Beanstalk with a multi-Docker container solution stack. Select immutable updates as a deployment strategy. Select enhanced health as a monitoring type in the Elastic Beanstalk environment to ensure health checks aretransmitted at deployment.
B. Use an Amazon ECS cluster and service with an Application Load Balancer and an AWS CodeDeploy blue/green deployment type. Define a production port and a test port in Amazon ECS. Write an AWS Lambda function to test theapplication, and reference it within the AfterAllowTestTraffic hook in the appspec.yml.
C. Use AWS CloudFormation to provision Amazon EC2 instances behind an Application Load Balancer. Deploy the containers using Amazon ECS. Upon deployment, replicate the configuration in the new EC2 instances, perform testing,and switch traffic from the old Application Load Balancer to the new one using Amazon Route 53.
D. Use an Amazon ECS cluster and service along with Amazon EC2 instances and an Application Load Balancer. Select rolling update as a deployment strategy. Add a Docker health check within the task definition to ensure rollback if thehealth check fails.

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



**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/compute/bluegreen-deployments-with-amazon-ecs/

**QUESTION 196**
A company is using Amazon EC2 for various workloads. Company policy requires that instances be managed centrally to standardize configurations. These configurations include standard logging, metrics, security assessments, and weekly patching.
How can the company meet these requirements? (Choose three.)

A. Use AWS Config to ensure all EC2 instances are managed by Amazon Inspector.
B. Use AWS Config to ensure all EC2 instances are managed by AWS Systems Manager.
C. Use AWS Systems Manager to install and manage Amazon Inspector, Systems Manager Patch Manager, and the Amazon CloudWatch agent on all instances.
D. Use Amazon Inspector to install and manage AWS Systems Manager, Systems Manager Patch Manager, and the Amazon CloudWatch agent on all instances.
E. Use AWS Systems Manager maintenance windows with Systems Manager Run Command to schedule Systems Manager Patch Manager tasks. Use the Amazon CloudWatch agent to schedule Amazon Inspector assessment runs.
F. Use AWS Systems Manager maintenance windows with Systems Manager Run Command to schedule Systems Manager Patch Manager tasks. Use Amazon

CloudWatch Events to schedule Amazon Inspector assessment runs.

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

**Explanation/Reference:**

**QUESTION 197**
A company has built a web service that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company has deployed the application in us-east-1. Amazon Route 53 provides an external DNS that routes traffic from example.com to the application, created with appropriate health checks.
The company has deployed a second environment for the application in eu-west-1. The company wants traffic to be routed to whichever environment results in the best response time for each user. If there is an outage in one Region, traffic should be directed to the other environment.
Which configuration will achieve these requirements?

A.
- A subdomain us.example.com with weighted routing: the US ALB with weight 2 and the EU ALB with weight 1.
- Another subdomain eu.example.com with weighted routing: the EU ALB with weight 2 and the US ALB with weight 1.
- Geolocation routing records for example.com: North America aliased to us.example.com and Europe aliased to eu.example.com.

B.
- A subdomain us.example.com with latency-based routing: the US ALB as the first target and the EU ALB as the second target.
- Another subdomain eu.example.com with latency-based routing: the EU ALB as the first target and the US ALB as the second target.
- Failover routing records for example.com aliased to us.example.com as the first target and eu.example.com as the second target.

C.
- A subdomain us.example.com with failover routing: the US ALB as primary and the EU ALB as secondary.
- Another subdomain eu.example.com with failover routing: the EU ALB as primary and the US ALB as secondary.
- Latency-based routing records for example.com that are aliased to us.example.com and eu.example.com.

D.
- A subdomain us.example.com with multivalue answer routing: the US ALB first and the EU ALB second.
- Another subdomain eu.example.com with multivalue answer routing: the EU ALB first and the US ALB second.
- Failover routing records for example.com that are aliased to us.example.com and eu.example.com.

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

**Explanation/Reference:**

**QUESTION 198**
A company hosts its staging website using an Amazon EC2 instance backed with Amazon EBS storage. The company wants to recover quickly with minimal data losses in the event of network connectivity issues or power failures on the EC2 instance.
Which solution will meet these requirements?

A. Add the instance to an EC2 Auto Scaling group with the minimum, maximum, and desired capacity set to 1.
B. Add the instance to an EC2 Auto Scaling group with a lifecycle hook to detach the EBS volume when the EC2 instance shuts down or terminates.
C. Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric and select the EC2 action to recover the instance.
D. Create an Amazon CloudWatch alarm for the StatusCheckFailed_Instance metric and select the EC2 action to reboot the instance.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-maintain-instance-levels.html

**QUESTION 199**
A company has a legacy application running on AWS. The application can only run on one Amazon EC2 instance at a time. Application metadata is stored in Amazon S3 and must be retrieved if the instance is restarted. The instance should be automatically restarted or relaunched if performance degrades.
Which solution will satisfy these requirements?

A. Create an Amazon CloudWatch alarm to monitor the EC2 instance. When the StatusCheckFailed system alarm is triggered, use the recover action to stop and start the instance. Use a trigger in Amazon S3 to push the metadata to theinstance when it is back up and running.
B. Use the auto healing feature in AWS OpsWorks to stop and start the EC2 instance. Use a lifecycle event in OpsWorks to pull the data from Amazon S3 and update it on the instance.
C. Use the Auto Recovery feature in Amazon EC2 to automatically stop and start the EC2 instance in case of a failure. Use a trigger in Amazon S3 to push the metadata to the instance when it is back up and running.
D. Use AWS CloudFormation to create an EC2 instance that includes the user-data property for the EC2 resource. Add a command in user-data to retrieve the application metadata from Amazon S3.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html

**QUESTION 200**
A company wants to migrate a legacy application to AWS and develop a deployment pipeline that uses AWS services only. A DevOps engineer is migrating all of the application code from a Git repository to AWS CodeCommit while preserving the history of the repository. The DevOps engineer has set all the permissions within CodeCommit, installed the Git client and the AWS CLI on a local computer, and is ready to migrate the repository.
Which actions will follow?

A. Create the CodeCommit repository using the AWS CLI. Clone the Git repository directly to CodeCommit using the AWS CLI. Validate that the files were migrated, and publish the CodeCommit repository.
B. Create the CodeCommit repository using the AWS Management Console. Clone both the Git and CodeCommit repositories to the local computer. Copy the files from the Git repository to the CodeCommit repository on the localcomputer. Commit the CodeCommit repository. Validate that the files were migrated, and share the CodeCommit repository.
C. Create the CodeCommit repository using the AWS Management Console. Use the console to clone the Git repository into the CodeCommit repository. Validate that the files were migrated, and publish the CodeCommit repository.
D. Create the CodeCommit repository using the AWS Management Console or the AWS CLI. Clone the Git repository with a mirror argument to the local computer and push the repository to CodeCommit. Validate that the files were migrated, and share the CodeCommit repository.

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

**Explanation/Reference:**

**QUESTION 201**
A company's security team discovers that IAM access keys were exposed in a public code repository. Moving forward, the DevOps team wants to implement a solution that will automatically disable any keys that are suspected of being compromised, and notify the security team.
Which solution will accomplish this?

A. Create an Amazon CloudWatch Events event for Amazon Macie. Create an Amazon SNS topic with two subscriptions: one to notify the security team and another to trigger an AWS Lambda function that disables the access keys.
B. Enable Amazon GuardDuty and set up an Amazon CloudWatch Events rule event for GuardDuty. Trigger an AWS Lambda function to check if the event relates to compromised keys. If so, send a notification to the security team anddisable the access keys.
C. Run an AWS CloudWatch Events rule every 5 minutes to invoke an AWS Lambda function that checks to see if the compromised tag for any access key is set to true. If so, notify the security team and disable the access keys.
D. Set up AWS Config and create an AWS CloudTrail event for AWS Config. Create an Amazon SNS topic with two subscriptions: one to notify the security team and another to trigger an AWS Lambda function that disables the accesskeys.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/RunLambdaSchedule.html

**QUESTION 202**
A company has mandated a global encryption-at-rest policy. A DevOps engineer has been tasked to ensure that new data uploaded to both new and existing Amazon S3 buckets is encrypted at rest across the company's AWS
Organizations organization. There are a number of legacy applications deployed on AWS that use Amazon S3 and do not store data encrypted at rest. These applications MUST continue to operate. The engineer must ensure S3 encryption at rest across the organization without requiring an application code change. How should this be accomplished with MINIMAL effort?

A. Develop an AWS Lambda function that lists all Amazon S3 buckets in a given account and applies default encryption to all S3 buckets that either do not have it enabled or to those with an S3 bucket policy that do not explicitly deny putobject requests without server-side encryption. Deploy the Lambda function along with an Amazon EventBridge (Amazon CloudWatch Events) scheduled rule with AWS CloudFormation StackSets to all accounts within the organization.
B. Enable the AWS Config s3-bucket-server-side-encryption-enabled managed rule that checks for S3 bucket that either do not have S3 default encryption enabled or those with an S3 bucket policy that does not explicitly deny put-object requests without server-side encryption. Add the AWS-EnabledS3BucketEncryption remediation action to the AWS Config rule to enable default encryption on any S3 buckets that are not complaint. Use AWS Config organizations integration to deploy the rule across all accounts in the organization.
C. Enable an AWS Config custom rule that checks for S3 buckets that do not have a bucket policy denying access to s3:PutObject unless the x-amz-server-side-encryption S3 condition is met with an AES 256 value or x-amz-server-side-encryption is not present. Add a custom remediation action to the AWS Config rule that will apply the bucket policy if the S3 bucket is non-complaint. Use AWS Config organizations integration to deploy the rule across all accounts in the organization.
D. Write an SCP that denies access to s3:PutObject unless either the x-amz-server-side-encryption S3 condition is met with an AES 256 value or x-amz-server-side-encryption is not present. Apply the SCP to the root of the organization toenforce the policy across the entire organization.



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

**Explanation/Reference:**

**QUESTION 203**
A DevOps engineer is assisting with a multi-Region disaster recovery solution for a new application. The application consists of Amazon EC2 instances running in an Auto Scaling group and an Amazon Aurora MySQL DB cluster. The application must be available with an RTO of 120 minutes and an RPO of 60 minutes. What is the MOST cost-effective way to meet these requirements?

A. Launch an Aurora DB cluster as an Aurora Replica in a different Region. Create an AWS CloudFormation template for all compute resources and create a stack in two Regions. Write a script that promotes the Aurora Replica to theprimary instance in the event of a failure.
B. Launch an Aurora DB cluster as an Aurora Replica in a different Region and configure automatic cross-Region failover. Create an AWS CloudFormation template that includes an Auto Scaling group, and create a stack in two Regions.Write a script that updates the CloudFormation stack in the disaster recovery Region to increase the number of instances.
C. Use AWS Lambda to create and copy a snapshot of the Aurora DB cluster to the destination Region hourly. Create an AWS CloudFormation template that includes an Auto Scaling group, and create a stack in two Regions. Restore theAurora DB cluster from a snapshot and update the Auto Scaling group to start

launching instances.

D. Configure Amazon DynamoDB cross-Region replication. Create an AWS CloudFormation template that includes an Auto Scaling group, and create a stack in two Regions. Write a script that will update the CloudFormation stack in thedisaster recovery Region and promote the DynamoDB replica to the primary instance in the event of a failure.

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

**Explanation/Reference:**

**QUESTION 204**
A company that runs many workloads on AWS has an Amazon EBS spend that has increased over time. The DevOps team notices there are many unattached EBS volumes. Although there are workloads where volumes are detached, volumes over 14 days old are stale and no longer needed. A DevOps engineer has been tasked with creating automation that deletes unattached EBS volumes that have been unattached for 14 days.
Which solution will accomplish this?

A. Configure the AWS Config ec2-volume-inuse-check managed rule with a configuration changes trigger type and an Amazon EC2 volume resource target. Create a new Amazon CloudWatch Events rule scheduled to execute an AWSLambda function in 14 days to delete the specified EBS volume.

B. Use Amazon EC2 and Amazon Data Lifecycle Manager to configure a volume lifecycle policy. Set the interval period for unattached EBS volumes to 14 days and set the retention rule to delete. Set the policy target volumes as *.

C. Create an Amazon CloudWatch Events rule to execute an AWS Lambda function daily. The Lambda function should find unattached EBS volumes and tag them with the current date, and delete unattached volumes that have tags withdates that are more than 14 days old.

D. Use AWS Trusted Advisor to detect EBS volumes that have been detached for more than 14 days. Execute an AWS Lambda function that creates a snapshot and then deletes the EBS volume.

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

**Explanation/Reference:**

**QUESTION 205**
A DevOps engineer is troubleshooting deployments to a new application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones.
Instances sometimes come online before they are ready, which is leading to increased error rates among users. The current health check configuration gives instances a 60-second grace period and considers instances healthy after two 200 response codes from /index.php, a page that may respond intermittently during the deployment process. The development team wants instances to come online as soon as possible.

Which strategy would address this issue?

A. Increase the instance grace period from 60 seconds to 180 seconds, and the consecutive health check requirement from 2 to 3.
B. Increase the instance grace period from 60 second to 120 seconds, and change the response code requirement from 200 to 204.
C. Modify the deployment script to create a /health-check.php file when the deployment begins, then modify the health check path to point to that file.
D. Modify the deployment script to create a /health-check.php file when all tasks are complete, then modify the health check path to point to that file.

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

**Explanation/Reference:**

**QUESTION 206**
A DevOps team manages an API running on-premises that serves as a backend for an Amazon API Gateway endpoint. Customers have been complaining about high response latencies, which the development team has verified using the API Gateway latency metrics in Amazon CloudWatch. To identify the cause, the team needs to collect relevant data without introducing additional latency.
Which actions should be taken to accomplish this? (Choose two.)

A. Install the CloudWatch agent server side and configure the agent to upload relevant logs to CloudWatch.
B. Enable AWS X-Ray tracing in API Gateway, modify the application to capture request segments, and upload those segments to X-Ray during each request.
C. Enable AWS X-Ray tracing in API Gateway, modify the application to capture request segments, and use the X-Ray daemon to upload segments to X-Ray.
D. Modify the on-premises application to send log information back to API Gateway with each request.
E. Modify the on-premises application to calculate and upload statistical data relevant to the API service requests to CloudWatch metrics.

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

**Explanation/Reference:**

**QUESTION 207**
A devops team uses AWS CloudFormation to build their infrastructure. The security team is concerned about sensitive parameters, such as passwords, being exposed.
Which combination of steps will enhance the security of AWS CloudFormation? (Choose three.)

A. Create a secure string with AWS KMS and choose a KMS encryption key. Reference the ARN of the secure string, and give AWS CloudFormation permission

to the KMS key for decryption.

B. Create secrets using the AWS Secrets Manager AWS::SecretsManager::Secret resource type. Reference the secret resource return attributes in resources that need a password, such as an Amazon RDS database.

C. Store sensitive static data as secure strings in the AWS Systems Manager Parameter Store. Use dynamic references in the resources that need access to the data.

D. Store sensitive static data in the AWS Systems Manager Parameter Store as strings. Reference the stored value using types of Systems Manager parameters.

E. Use AWS KMS to encrypt the CloudFormation template.

F. Use the CloudFormation NoEcho parameter property to mask the parameter value.

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

**Explanation/Reference:**

**QUESTION 208**
A company wants to ensure that their EC2 instances are secure. They want to be notified if any new vulnerabilities are discovered on their instances, and they also want an audit trail of all login activities on the instances.
Which solution will meet these requirements?



A. Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Amazon Kinesis Agent to capture system logs and deliver them to Amazon S3.

B. Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Systems Manager Agent to capture system logs and view login activity in the CloudTrail console.

C. Configure Amazon CloudWatch to detect vulnerabilities on the EC2 instances. Install the AWS Config daemon to capture system logs and view them in the AWS Config console.

D. Configure Amazon Inspector to detect vulnerabilities on the EC2 instances. Install the Amazon CloudWatch Agent to capture system logs and record them via Amazon CloudWatch Logs.

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

**Explanation/Reference:**

**QUESTION 209**

A development team is using AWS CodeCommit to version control application code and AWS CodePipeline to orchestrate software deployments. The team has decided to use a remote master branch as the trigger for the pipeline to integrate code changes. A developer has pushed code changes to the CodeCommit repository, but noticed that the pipeline had no reaction, even after 10 minutes.
Which of the following actions should be taken to troubleshoot this issue?

A. Check that an Amazon CloudWatch Events rule has been created for the master branch to trigger the pipeline.
B. Check that the CodePipeline service role has permission to access the CodeCommit repository.
C. Check that the developer's IAM role has permission to push to the CodeCommit repository.
D. Check to see if the pipeline failed to start because of CodeCommit errors in Amazon CloudWatch Logs.

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

**Explanation/Reference:**

**QUESTION 210**
A company has multiple development teams sharing one AWS account. The development team's manager wants to be able to automatically stop Amazon EC2 instances and receive notifications if resources are idle and not tagged as production resources.
Which solution will meet these requirements?



A. Use a scheduled Amazon CloudWatch Events rule to filter for Amazon EC2 instance status checks and identify idle EC2 instances. Use the CloudWatch Events rule to target an AWS Lambda function to stop non-production instancesand send notifications.
B. Use a scheduled Amazon CloudWatch Events rule to filter AWS Systems Manager events and identify idle EC2 instances and resources. Use the CloudWatch Events rule to target an AWS Lambda function to stop non-productioninstances and send notifications.
C. Use a scheduled Amazon CloudWatch Events rule to target a custom AWS Lambda function that runs AWS Trusted Advisor checks. Create a second CloudWatch Events rule to filter events from Trusted Advisor to trigger a Lambdafunction to stop idle non-production instances and send notifications.
D. Use a scheduled Amazon CloudWatch Events rule to target Amazon Inspector events for idle EC2 instances. Use the CloudWatch Events rule to target the AWS Lambda function to stop non-production instances and send notifications.

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

**Explanation/Reference:**

**QUESTION 211**

A company is migrating its public-facing software to AWS. The company plans to use Amazon EC2 to run application code and Amazon RDS to store all application data. The company wants to primarily use one Region with failover capabilities to a secondary Region and Amazon Route 53 to route traffic. The RPO is 2 hours and the RTO is 4 hours.
Which combination of steps should be used to meet these requirements while MINIMIZING cost? (Choose three.)

A. Create an AWS CloudFormation template to provision the application server and database instance in a single Region.
B. Create an AWS CloudFormation template to provision the application tier of the application and a multi-Region database instance.
C. Configure Amazon CloudWatch Events rules to run every hour. Trigger AWS Lambda functions to create an RDS snapshot and copy it to the secondary Region.
D. Configure Amazon CloudWatch Events rules to run every 3 hours. Trigger AWS Lambda functions to create an RDS snapshot and copy it to the secondary Region.
E. In the event of a failure, deploy a new AWS CloudFormation stack in a secondary region to provision the application resources and a new RDS instance using the copied snapshot and a Route 53 failover routing policy.
F. In the event of a failure, deploy a new AWS CloudFormation stack in a secondary region to provision the application resources and a replica of the RDS database using the copied snapshot and a Route 53 latency-based routing policy.

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

**Explanation/Reference:**



**QUESTION 212**
A DevOps engineer wants to find a solution to migrate an application from on premises to AWS. The application is running on Linux and needs to run on specific versions of Apache Tomcat, HAProxy, and Varnish Cache to function properly. The application's operating system-level parameters require tuning. The solution must include a way to automate the deployment of new application versions. The infrastructure should be scalable and faulty servers should be replaced automatically.
Which solution should the DevOps engineer use?

A. Upload the application as a Docker image that contains all the necessary software to Amazon ECR. Create an Amazon ECS cluster using an AWS Fargate launch type and an Auto Scaling group. Create an AWS CodePipeline pipelinethat uses Amazon ECR as a source and Amazon ECS as a deployment provider.
B. Upload the application code to an AWS CodeCommit repository with a saved configuration file to configure and install the software. Create an AWS Elastic Beanstalk web server tier and a load balanced-type environment that uses theTomcat solution stack. Create an AWS CodePipeline pipeline that uses CodeCommit as a source and Elastic Beanstalk as a deployment provider.
C. Upload the application code to an AWS CodeCommit repository with a set of .ebextensions files to configure and install the software. Create an AWS Elastic Beanstalk worker tier environment that uses the Tomcat solution stack. Createan AWS CodePipeline pipeline that uses CodeCommit as a source and Elastic Beanstalk as a deployment provider.

D. Upload the application code to an AWS CodeCommit repository with an appspec.yml file to configure and install the necessary software. Create an AWS CodeDeploy deployment group associated with an Amazon EC2 Auto Scalinggroup. Create an AWS CodePipeline pipeline that uses CodeCommit as a source and CodeDeploy as a deployment provider.

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

**Explanation/Reference:**

**QUESTION 213**
A company wants to use AWS CloudFormation for infrastructure deployment. The company has strict tagging and resource requirements and wants to limit the deployment to two Regions. Developers will need to deploy multiple versions of the same application.
Which solution ensures resources are deployed in accordance with company policy?

A. Create AWS Trusted Advisor checks to find and remediate unapproved CloudFormation StackSets.
B. Create a CloudFormation drift detection operation to find and remediate unapproved CloudFormation StackSets.
C. Create CloudFormation StackSets with approved CloudFormation templates.
D. Create AWS Service Catalog products with approved CloudFormation templates.



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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/aws/use-cloudformation-stacksets-to-provision-resources-across-multiple-aws-accounts-and-regions/

**QUESTION 214**
A company is deploying a new application using Amazon EC2 instances. The company wants to maintain a centralized application and Amazon API logs that can be queried using one tool or service.
Which solution will meet these requirements?

A. Use the Amazon CloudWatch agent to send logs from the Amazon EC2 instances to CloudWatch. Configure AWS CloudTrail to deliver the API logs to CloudWatch and use Amazon Athena to query both log sets in CloudWatch.
B. Use the Amazon CloudWatch agent to send logs from the Amazon EC2 instances to CloudWatch. Configure an Amazon Kinesis Data Firehouse log group subscription to send those logs to Amazon S3. Use AWS CloudTrail to deliver theAPI logs to Amazon S3. Use Amazon Athena to query both log sets in Amazon S3.
C. Use the Amazon CloudWatch agent to send logs from the Amazon EC2 instances to Amazon Kinesis. Configure AWS CloudTrail to deliver the API logs to

Kinesis. Use Amazon to load the data into Amazon Redshift and use AmazonRedshift to query both log sets.

D. Use the Amazon CloudWatch agent to send logs from the Amazon EC2 instances to Amazon S3. Use Amazon CloudTrail to deliver the API logs to Amazon S3 and use Amazon Redshift to query both log sets in Amazon S3.

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

**Explanation/Reference:**

**QUESTION 215**
A company requires that its internally facing web application be highly available. The architecture is made up of one Amazon EC2 web server instance and one NAT instance that provides outbound internet access for updates and accessing public data.
Which combination of architecture adjustments should the company implement to achieve high availability? (Choose two.)

A. Add the NAT instance to an EC2 Auto Scaling group that spans multiple Availability Zones. Update the route tables.

B. Create additional EC2 instances spanning multiple Availability Zones. Add an Application Load Balancer to split the load between them.

C. Configure an Application Load Balancer in front of the EC2 instance. Configure Amazon CloudWatch alarms to recover the EC2 instance upon host failure.

D. Replace the NAT instance with a NAT gateway in each Availability Zone. Update the route tables.

E. Replace the NAT instances with a NAT gateway that spans multiple Availability Zones. Update the route tables.



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

**Explanation/Reference:**

**QUESTION 216**
A company is required to collect user consent to a privacy agreement. An application is deployed in six AWS Regions with two in North America, two in Europe, and two in Asia with a user base of 20-30 million users. The company needs to read and write data related to each user's response, and ensure the responses are available in all six Regions.
What solution will satisfy these requirements while MINIMIZING latency?

A. Implement Amazon Aurora Global Database in each of the six Regions.

B. Implement Amazon DocumentDB (with MongoDB compatibility) in each of the six Regions.

C. Implement Amazon DynamoDB global tables in each of the six Regions.

D. Implement Amazon ElastiCache for Redis replication group in each of the six Regions.

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

**Explanation/Reference:**

**QUESTION 217**
A company updated the AWS CloudFormation template for a critical business application. The stack update process failed due to an error in the updated template, and CloudFormation automatically began the stack rollback process. Later, a DevOps engineer found the application was still unavailable, and that the stack was in the UPDATE_ROLLBACK_FAILED state.
Which combination of actions will allow the stack rollback to complete successfully? (Choose two.)

A. Attach the AWSCloudFormationFullAccess IAM policy to the CloudFormation role.
B. Automatically heal the stack resources using CloudFormation drift detection.
C. Issue a ContinueUpdateRollback command from the CloudFormation console or AWS CLI.
D. Manually adjust the resources to match the expectations of the stack.
E. Update the existing CloudFormation stack using the original template.



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

**Explanation/Reference:**
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/cloudformation-update-rollback-failed/

**QUESTION 218**
A company has multiple child accounts that are part of an organization in AWS Organizations. The security team needs to review every Amazon EC2 security group and their inbound and outbound rules. The security team wants to programmatically retrieve this information from the child accounts using an AWS Lambda function in the master account of the organization.
Which combination of access changes will meet these requirements? (Choose three.)

A. Create a trust relationship that allows users in the child accounts to assume the master account IAM role.
B. Create a trust relationship that allows users in the master account to assume the IAM roles of the child accounts.
C. Create an IAM role in each child account that has access to the AmazonEC2ReadOnlyAccess managed policy.
D. Create an IAM role in each child account to allow the sts:AssumeRole action against the master account IAM role's ARN.
E. Create an IAM role in the master account that allows the sts:AssumeRole action against the child account IAM role's ARN.
F. Create an IAM role in the master account that has access to the AmazonEC2ReadOnlyAccess managed policy.

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

**Explanation/Reference:**

**QUESTION 219**
A DevOps engineer notices that all Amazon EC2 instances running behind an Application Load Balancer in an Auto Scaling group are failing to respond to user requests. The EC2 instances are also failing target group HTTP health checks.
Upon inspection, the engineer notices the application process was not running in any EC2 instances. There are a significant number of out of memory messages in the system logs. The engineer needs to improve the resilience of the application to cope with a potential application memory leak. Monitoring and notifications should be enabled to alert when there is an issue.
Which combination of actions will meet these requirements? (Choose two.)

A. Change the Auto Scaling configuration to replace the instances when they fail the load balancer's health checks.
B. Change the target group health check HealthCheckIntervalSeconds parameter to reduce the interval between health checks.
C. Change the target group health checks from HTTP to TCP to check if the port where the application is listening is reachable.
D. Enable the available memory consumption metric within the Amazon CloudWatch dashboard for the entire Auto Scaling group. Create an alarm when the memory utilization is high. Associate an Amazon SNS topic to the alarm toreceive notifications when the alarm goes off.
E. Use the Amazon CloudWatch agent to collect the memory utilization of the EC2 instances in the Auto Scaling group. Create an alarm when the memory utilization is high and associate an Amazon SNS topic to receive a notification.

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

**Explanation/Reference:**

**QUESTION 220**
A developer is building an application that must allow users to upload images to an Amazon S3 bucket. Users need to be able to sign in to the application using Facebook to upload images.
How can these requirements be met?

A. Store a user's Facebook user name and password in an Amazon DymanoDB table. Authenticate against those credentials the next time the user tries to log in.
B. Create an Amazon Cognito identity pool using Facebook as the identity provider. Obtain temporary AWS credentials so a user can access Amazon S3.
C. Create multiple AWS IAM users. Set the email and password to be the same as each user's Facebook login credentials.

D. Create a new Facebook account and store its login credentials in an S3 bucket. Share that S3 bucket with a user. The user will log in to the application using those retrieved credentials.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/mobile/store-your-photos-in-the-cloud-using-amazon-s3/

**QUESTION 221**
An application running on multiple Amazon EC2 instances pulls messages from a standard Amazon SQS queue. A requirement for the application is that all messages must be encrypted at rest.
Developers are instructed to use methods that allow for centralized key management and minimize possible support requirements whenever possible.
Which of the following solutions supports these requirements?

A. Encrypt individual messages by using client-side encryption with customer managed keys, then write to the SQS queue.
B. Encrypt individual messages by using SQS Extended Client and the Amazon S3 encryption client.
C. Create an SQS queue, and encrypt the queue by using server-side encryption with AWS KMS.
D. Create an SQS queue, and encrypt the queue by using client-side encryption.



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

**Explanation/Reference:**

**QUESTION 222**
A developer tested an application locally and then deployed it to AWS Lambda. While testing the application remotely, the Lambda function fails with an access denied message.
How can this issue be addressed?

A. Update the Lambda function's execution role to include the missing permissions.
B. Update the Lambda function's resource policy to include the missing permissions.
C. Include an IAM policy document at the root of the deployment package and redeploy the Lambda function.
D. Redeploy the Lambda function using an account with access to the AdministratorAccess policy.

**Correct Answer:** A

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/access-denied-lambda-s3-bucket/

**QUESTION 223**
The development team is creating a social media game which ranks users on a scoreboard. The current implementation uses an Amazon RDS for MySQL database for storing user data; however, the game cannot display scores quickly enough during performance testing.
Which service would provide the fastest retrieval times?

A. Migrate user data to Amazon DynamoDB for managing content.
B. Use AWS Batch to compute and deliver user and score content.
C. Deploy Amazon CloudFront for user and score content delivery.
D. Set up Amazon ElastiCache to deliver user and score content.

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

**Explanation/Reference:**



**QUESTION 224**
A developer has written an application that writes data to Amazon DynamoDB. The DynamoDB table has been configured to use conditional writes. During peak usage times, writes are failing due to a ConditionalCheckFailedException error.
How can the developer increase the application's reliability when multiple clients are attempting to write to the same record?

A. Write the data to an Amazon SNS topic.
B. Increase the amount of write capacity for the table to anticipate short-term spikes or bursts in write operations.
C. Implement a caching solution, such as DynamoDB Accelerator or Amazon ElastiCache.
D. Implement error retries and exponential backoff with jitter.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-table-throttled/

**QUESTION 225**
A company uses federated access for its AWS environment. The available roles are created and managed using AWS CloudFormation from CI/CD pipeline. All changes should be made to the IAM roles through the pipeline. The security team found that changes are being made to the roles out-of-band and would like to detect when this occurs.
Which action will accomplish this?

A. Use Amazon Inspector rules to detect and notify when a CloudFormation stack has a configuration change.
B. Use an AWS Trusted Advisor CloudWatch Events rule to detect and notify when a CloudFormation stack has a configuration change.
C. Use AWS CloudTrail to detect and notify when a CloudFormation stack has detected a configuration change.
D. Use an AWS Config rule to detect and notify when a CloudFormation stack has detected a configuration change.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/mt/how-to-track-configuration-changes-to-cloudformation-stacks-using-aws-config/

**QUESTION 226**
An application running on a set of Amazon EC2 instances in an Auto Scaling group requires a configuration file to operate. The instances are created and maintained with AWS CloudFormation. A DevOps engineer wants the instances to have the latest configuration file when launched, and wants changes to the configuration file to be reflected on all the instances with a minimal delay when the CloudFormation template is updated. Company policy requires that application configuration files be maintained along with AWS infrastructure configuration files in source control.
Which solution will accomplish this?

A. In the CloudFormation template, add an AWS Config rule. Place the configuration file content in the rule's InputParameters property, and set the Scope property to the EC2 Auto Scaling group. Add an AWS Systems Manager ResourceData Sync resource to the template to poll for updates to the configuration.
B. In the CloudFormation template, add an EC2 launch template resource. Place the configuration file content in the launch template. Configure the cfn-init script to run when the instance is launched, and configure the cfn-hup script to pollfor updates to the configuration.
C. In the CloudFormation template, add an EC2 launch template resource. Place the configuration file content in the launch template. Add an AWS Systems Manager Resource Data Sync resource to the template to poll for updates to theconfiguration.
D. In the CloudFormation template, add Cloud Formation init metadata. Place the configuration file content in the metadata. Configure the cfn-init script to run when the instance is launched, and configure the cfn-hup script to poll forupdates to the configuration.

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

**Explanation/Reference:**

**QUESTION 227**
A company is using AWS CodeCommit as its source code repository. After an internal audit, the compliance team mandates that any code change that go into the master branch must be committed by senior developers.
Which solution will meet these requirements?

A. Create two repositories in CodeCommit: one for working and another for the master. Create separate IAM groups for senior developers and developers. Assign the resource-level permissions on the repositories tied to the IAM groups.After the code changes are reviewed, sync the approved files to the master code commit repository.
B. Create a repository in CodeCommit. Create separate IAM groups for senior developers and developers. Assign code commit permissions for both groups, with code merge permissions for the senior developers group. Create a trigger tonotify senior developers with a URL link to approve or deny commit requests delivered through Amazon SNS. Once a senior developer approves the code, the code gets merged to the master branch.
C. Create a repository in CodeCommit with a working and master branch. Create separate IAM groups for senior developers and developers. Use an IAM policy to assign each IAM group their corresponding branches. Once the code ismerged to the working branch, senior developers can pull the changes from the working branch to the master branch.
D. Create a repository in CodeCommit. Create separate IAM groups for senior developers and developers. Use AWS Lambda triggers on the master branch and get the user name of the developer at the event object of the Lambda function.Validate the user name with the IAM group to approve or deny the commit.



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

**Explanation/Reference:**

**QUESTION 228**
A DevOps engineer used an AWS CloudFormation custom resource to set up AD Connector. The AWS Lambda function executed and created AD Connector, but CloudFormation is not transitioning from CREATE_IN_PROGRESS to
CREATE_COMPLETE.
Which action should the engineer take to resolve this issue?

A. Ensure the Lambda function code has exited successfully.
B. Ensure the Lambda function code returns a response to the pre-signed URL.
C. Ensure the Lambda function IAM role has cloudformation:UpdateStack permissions for the stack ARN.
D. Ensure the Lambda function IAM role has ds:ConnectDirectory permissions for the AWS account.

**Correct Answer:** B

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

**Explanation/Reference:**
Section: (none)

**QUESTION 229**
A DevOps engineer is tasked with creating a more stable deployment solution for a web application in AWS. Previous deployments have resulted in user-facing bugs, premature user traffic, and inconsistencies between web servers running behind an Application Load Balancer. The current strategy uses AWS CodeCommit to store the code for the application. When developers push to the master branch of the repository, CodeCommit triggers an AWS Lambda deploy function, which invokes an AWS Systems Manager run command to build and deploy the new code to all Amazon EC2 instances. Which combination of actions should be taken to implement a more stable deployment solution? (Choose two.)

A. Create a pipeline in AWS CodePipeline with CodeCommit as a source provider. Create parallel pipeline stages to build and test the application. Pass the build artifact to AWS CodeDeploy.
B. Create a pipeline in AWS CodePipeline with CodeCommit as a source provider. Create separate pipeline stages to build and then test the application. Pass the build artifact to AWS CodeDeploy.
C. Create and use an AWS CodeDeploy application and deployment group to deploy code updates to the EC2 fleet. Select the Application Load Balancer for the deployment group.
D. Create individual Lambda functions to run all build, test, and deploy actions using AWS CodeDeploy instead of AWS Systems Manager.
E. Modify the Lambda function to build a single application package to be shared by all instances. Use AWS CodeDeploy instead of AWS Systems Manager to update the code on the EC2 fleet.

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

**Explanation/Reference:**

**QUESTION 230**
A company uses AWS Storage Gateway in file gateway mode in front of an Amazon S3 bucket that is used by multiple resources. In the morning when business begins, users do not see the objects processed by a third party the previous evening. When a DevOps engineer looks directly at the S3 bucket, the data is there, but it is missing in Storage Gateway.
Which solution ensures that all the updated third-party files are available in the morning?

A. Configure a nightly Amazon EventBridge (Amazon CloudWatch Events) event to trigger an AWS Lambda function to run the RefreshCache command for Storage Gateway.
B. Instruct the third party to put data into the S3 bucket using AWS Transfer for SFTP.

C. Modify Storage Gateway to run in volume gateway mode.
D. Use S3 same-Region replication to replicate any changes made directly in the S3 bucket to Storage Gateway.

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

**Explanation/Reference:**

**QUESTION 231**
A company's legacy application uses IAM user credentials to access resources in the company's AWS Organizations organization. A DevOps engineer needs to ensure new IAM users cannot be created unless the employee creating the IAM user is on an exception list.
Which solution will meet these requirements?

A. Attach an Organizations SCP with an explicit deny for all iam:CreateAccessKey actions with a condition that excludes StringNotEquals for aws:username with a value of the exception list.
B. Attach an Organizations SCP with an explicit deny for all iam:CreateUser actions with a condition that includes StringEquals for aws:username with a value of the exception list.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with a pattern that matches the iam:CreateAccessKey action with an AWS Lambda function target. The function will check the user name account against an exceptionlist. If the user is not in the exception list, the function will delete the user.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with a pattern that matches the iam:CreateUser action with an AWS Lambda function target. The function will check the user name and account against an exceptionlist. If the user is not in the exception list, the function will delete the user.

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

**Explanation/Reference:**

**QUESTION 232**
A company has an application that is using a MySQL-compatible Amazon Aurora Multi-AZ DB cluster as the database. A cross-Region read replica has been created for disaster recovery purposes. A DevOps engineer wants to automate the promotion of the replica so it becomes the primary database instance in the event of a failure.
Which solution will accomplish this?

A. Configure a latency-based Amazon Route 53 CNAME with health checks so it points to both the primary and replica endpoints. Subscribe an Amazon SNS topic to Amazon RDS failure notifications from AWS CloudTrail and use thattopic to trigger an AWS Lambda function that will promote the replica instance as the master.

B. Create an Aurora custom endpoint to point to the primary database instance. Configure the application to use this endpoint. Configure AWS CloudTrail to run an AWS Lambda function to promote the replica instance and modify thecustom endpoint to point to the newly promoted instance.
C. Create an AWS Lambda function to modify the application's AWS Cloud Formation template to promote the replica, apply the template to update the stack, and point the application to the newly promoted instance. Create an AmazonCloudWatch alarm to trigger this Lambda function after the failure event occurs.
D. Store the Aurora endpoint in AWS Systems Manager Parameter Store. Create an Amazon EventBridge (Amazon CloudWatch Events) event that defects the database failure and runs an AWS Lambda function to promote the replicainstance and update the endpoint URL stored in AWS Systems Manager Parameter Store. Code the application to reload the endpoint from Parameter Store if a database connection fails.

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

**Explanation/Reference:**

**QUESTION 233**
A software company wants to automate the build process for a project where the code is stored in GitHub. When the repository is updated, source code should be compiled, tested, and pushed to Amazon S3. Which combination of steps would address these requirements? (Choose three.)

A. Add a buildspec.yml file to the source code with build instructions.
B. Configure a GitHub webhook to trigger a build every time a code change is pushed to the repository.
C. Create an AWS CodeBuild project with GitHub as the source repository.
D. Create an AWS CodeDeploy application with the Amazon EC2/On-Premises compute platform.
E. Create an AWS OpsWorks deployment with the install dependencies command.
F. Provision an Amazon EC2 instance to perform the build.

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

**Explanation/Reference:**

**QUESTION 234**
A DevOps engineer is deploying a new version of a company's application in an AWS CodeDeploy deployment group associated with its Amazon EC2 instances. After some time, the deployment fails. The engineer realizes that all the events associated with the specific deployment ID are in a Skipped status, and code was not deployed in the instances associated with the deployment group.
What are valid reasons for this failure? (Choose two.)

A. The networking configuration does not allow the EC2 instances to reach the internet via a NAT gateway or internet gateway, and the CodeDeploy endpoint cannot be reached.
B. The IAM user who triggered the application deployment does not have permission to interact with the CodeDeploy endpoint.
C. The target EC2 instances were not properly registered with the CodeDeploy endpoint.
D. An instance profile with proper permissions was not attached to the target EC2 instances.
E. The appspec.yml file was not included in the application revision.

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

**Explanation/Reference:**
Section: (none)

**QUESTION 235**
A company recently migrated its legacy application from on-premises to AWS. The application is hosted on Amazon EC2 instances behind an Application Load Balancer, which is behind Amazon API Gateway. The company wants to ensure users experience minimal disruptions during any deployment of a new version of the application. The company also wants to ensure it can quickly roll back updates if there is an issue.
Which solution will meet these requirements with MINIMAL changes to the application?



A. Introduce changes as a separate environment parallel to the existing one. Configure API Gateway to use a canary release deployment to send a small subset of user traffic to the new environment.
B. Introduce changes as a separate environment parallel to the existing one. Update the application's DNS alias records to point to the new environment.
C. Introduce changes as a separate target group behind the existing Application Load Balancer. Configure API Gateway to route user traffic to the new target group in steps.
D. Introduce changes as a separate target group behind the existing Application Load Balancer. Configure API Gateway to route all traffic to the Application Load Balancer, which then sends the traffic to the new target group.

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

**Explanation/Reference:**

**QUESTION 236**
A company runs an application consisting of an AWS CodeDeploy deployment group that uses Auto Scaling and an Application Load Balancer. The application deployments are automated using AWS CodePipeline, which consists of AWS CodeCommit as the source and AWS CodeDeploy as the deployment provider. After a recent successful deployment, the application experienced an outage for several minutes until the deployment was manually rolled back. A DevOps

engineer verified that the pipeline was successful and did not indicate any errors, but found that the code caused the application to become unresponsive after several hours.
Which actions will help to prevent future downtime in similar situations? (Choose two.)

A. Configure a TCP health check for the Auto Scaling target group on a listening port of the application.
B. Configure an HTTP or HTTPS health check for the Auto Scaling target group to check a specific application path.
C. Create a script to test the application health and execute the script during the BeforeInstall lifecycle hook in the CodeDeploy appspec.yml file.
D. Update the CodeDeploy deployment group to roll back automatically to the previous version if the deployment fails.
E. Update the CodeDeploy deployment group to roll back based on a custom Amazon CloudWatch alarm using an application status metric.

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

**Explanation/Reference:**

**QUESTION 237**
A DevOps engineer is deploying an AWS Service Catalog portfolio using AWS CodePipeline. The pipeline should create products and templates based on a manifest file in either JSON or YAML, and should enforce security requirements on all AWS Service Catalog products managed through the pipeline.
Which solution will meet the requirements in an automated fashion?



A. Use the AWS Service Catalog deploy action in AWS CodeDeploy to push new versions of products into the AWS Service Catalog with verification steps in the CodeDeploy AppSpec.
B. Use the AWS Service Catalog deploy action in AWS CodeBuild to verify and push new versions of products into the AWS Service Catalog.
C. Use an AWS Lambda action in CodePipeline to run a Lambda function to verify and push new versions of products into the AWS Service Catalog.
D. Use an AWS Lambda action in AWS CodeBuild to run a Lambda function to verify and push new versions of products into the AWS Service Catalog.

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

**Explanation/Reference:**

**QUESTION 238**
A company wants to use AWS Systems Manager documents to bootstrap physical laptops for developers. The bootstrap code is stored in GitHub. A DevOps engineer has already created a Systems Manager activation, installed the Systems Manager agent with the registration code, and installed an activation ID on all the laptops.

Which set of steps should be taken next?

A. Configure the Systems Manager document to use the AWS-RunShellScript command to copy the files from GitHub to Amazon S3, then use the aws-downloadContent plugin with a sourceType of S3.
B. Configure the Systems Manager document to use the aws-configurePackage plugin with an install action and point to the Git repository.
C. Configure the Systems Manager document to use the aws-downloadContent plugin with a sourceType of GitHub and sourceInfo with the repository details.
D. Configure the Systems Manager document to use the aws:softwareInventory plugin and run the script from the Git repository.

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

**Explanation/Reference:**

**QUESTION 239**
A company requires its internal business teams to launch resources through pre-approved AWS CloudFormation templates only. The security team requires automated monitoring when resources drift from their expected state.
Which strategy should be used to meet these requirements?



A. Allow users to deploy CloudFormation stacks using a CloudFormation service role only. Use CloudFormation drift detection to detect when resources have drifted from their expected state.
B. Allow users to deploy CloudFormation stacks using a CloudFormation service role only. Use AWS Config rules to detect when resources have drifted from their expected state.
C. Allow users to deploy CloudFormation stacks using AWS Service Catalog only. Enforce the use of a launch constraint. Use AWS Config rules to detect when resources have drifted from their expected state.
D. Allow users to deploy CloudFormation stacks using AWS Service Catalog only. Enforce the use of a template constraint. Use Amazon EventBridge (Amazon CloudWatch Events) notifications to detect when resources have drifted fromtheir expected state.

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

**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

**QUESTION 240**
A company requires an RPO of 2 hours and an RTP of 10 minutes for its data and application at all times. An application uses a MySQL database and Amazon EC2 web servers. The development team needs a strategy for failover and disaster recovery.

Which combination of deployment strategies will meet these requirements? (Choose two.)

A. Create an Amazon Aurora cluster in one Availability Zone across multiple Regions as the data store. Use Aurora's automatic recovery capabilities in the event of a disaster.
B. Create an Amazon Aurora global database in two Regions as the data store. In the event of a failure, promote the secondary Region as the master for the application.
C. Create an Amazon Aurora multi-master cluster across multiple Regions as the data store. Use a Network Load Balancer to balance the database traffic in different Regions.
D. Set up the application in two Regions and use Amazon Route 53 failover-based routing that points to the Application Load Balancers in both Regions. Use health checks to determine the availability in a given Region. Use Auto Scalinggroups in each Region to adjust capacity based on demand.
E. Set up the application in two Regions and use a multi-Region Auto Scaling group behind Application Load Balancers to manage the capacity based on demand. In the event of a disaster, adjust the Auto Scaling group's desired instancecount to increase baseline capacity in the failover Region.

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

**Explanation/Reference:**



**QUESTION 241**
A company has an application deployed using Amazon ECS with data stored in an Amazon DynamoDB table. The company wants the application to fail over to another Region in a disaster recovery scenario. The application must also efficiently recover from any accidental data loss events. The RPO for the application is 1 hour and the RTO is 2 hours.
Which highly available solution should a DevOps engineer recommend?

A. Change the configuration of the existing DynamoDB table. Enable this as a global table and specify the second Region that will be used. Enable DynamoDB point-in-time recovery.
B. Enable DynamoDB Streams for the table and create an AWS Lambda function to write the stream data to an S3 bucket in the second Region. Schedule a job for every 2 hours to use AWS Data Pipeline to restore the database to thefailover Region.
C. Export the DynamoDB table every 2 hours using AWS Data Pipeline to an Amazon S3 bucket in the second Region. Use Data Pipeline in the second Region to restore the export from S3 into the second DynamoDB table.
D. Use AWS DMS to replicate the data every hour. Set the original DynamoDB table as the source and the new DynamoDB table as the target.

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

**Explanation/Reference:**

**QUESTION 242**
A company is implementing a well-architected design for its globally accessible API stack. The design needs to ensure both high reliability and fast response times for users located in North America and Europe.

The API stack contains the following three tiers:

- Amazon API Gateway
- AWS Lambda
- Amazon DynamoDB

Which solution will meet the requirements?

A. Configure Amazon Route 53 to point to API Gateway APIs in North America and Europe using health checks. Configure the APIs to forward requests to a Lambda function in that Region. Configure the Lambda functions to retrieve andupdate the data in a DynamoDB table in the same Region as the Lambda function.
B. Configure Amazon Route 53 to point to API Gateway APIs in North America and Europe using latency-based routing and health checks. Configure the APIs to forward requests to a Lambda function in that Region. Configure the Lambdafunctions to retrieve and update the data in a DynamoDB global table.
C. Configure Amazon Route 53 to point to API Gateway in North America, create a disaster recovery API in Europe, and configure both APIs to forward requests to the Lambda functions in that Region. Retrieve the data from a DynamoDBglobal table. Deploy a Lambda function to check the North America API health every 5 minutes. In the event of a failure, update Route 53 to point to the disaster recovery API.
D. Configure Amazon Route 53 to point to API Gateway API in North America using latency-based routing. Configure the API to forward requests to the Lambda function in the Region nearest to the user. Configure the Lambda function toretrieve and update the data in a DynamoDB table.

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

**Explanation/Reference:**

**QUESTION 243**
A company wants to migrate its content sharing web application hosted on Amazon EC2 to a serverless architecture. The company currently deploys changes to its application by creating a new Auto Scaling group of EC2 instances and a new Elastic Load Balancer, and then shifting the traffic away using an Amazon Route 53 weighted routing policy.
For its new serverless application, the company is planning to use Amazon API Gateway and AWS Lambda. The company will need to update its deployment processes to work with the new application. It will also need to retain the ability to test new features on a small number of users before rolling the features out to the entire user base.
Which deployment strategy will meet these requirements?

A. Use AWS CDK to deploy API Gateway and Lambda functions. When code needs to be changed, update the AWS CloudFormation stack and deploy the new version of the APIs and Lambda functions. Use a Route 53 failover routingpolicy for the canary release strategy.
B. Use AWS CloudFormation to deploy API Gateway and Lambda functions using Lambda function versions. When code needs to be changed, update the CloudFormation stack with the new Lambda code and update the API versionsusing a canary release strategy. Promote the new version when testing is complete.
C. Use AWS Elastic Beanstalk to deploy API Gateway and Lambda functions. When code needs to be changed, delpoy a new version of the API and Lambda functions. Shift traffic gradually using an Elastic Beanstalk blue/greendeployment.
D. Use AWS OpsWorks to deploy API Gateway in the service layer and Lambda functions in a custom layer. When code needs to be changed, use OpsWorks to perform a blue/green deployment and shift traffic gradually.

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

**Explanation/Reference:**

**QUESTION 244**
After a recent audit, a company decided to implement a new disaster recovery strategy for its Amazon S3 data and its MySQL database running on Amazon EC2. Management wants the ability to recover to a secondary AWS Region with an RPO under 5 seconds and an RTO under 1 minute.
Which actions will meet the requirements while MINIMIZING operational overhead? (Choose two.)

A. Modify the application to write to both Regions at the same time when uploading objects to Amazon S3.
B. Migrate the database to an Amazon Aurora multi-master in the primary and secondary Regions.
C. Migrate the database to Amazon RDS with a read replica in the secondary Region.
D. Migrate to Amazon Aurora Global Database.
E. Set up S3 cross-Region replication with a replication SLA for the S3 buckets where objects are being put.

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

**Explanation/Reference:**
Reference: https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/

**QUESTION 245**
A DevOps engineer is scheduling legacy AWS KMS keys for deletion and has created a remediation AWS Lambda function that will re-enable a key if necessary. The engineer wants to automate this process with available AWS CloudTrail data so, if a key scheduled for deletion is in use, it will be re-enabled.

Which solution enables this automation?

A. Create an Amazon CloudWatch Logs metric filter and alarm for KMS events with an error message. Set the remediation Lambda function as the target of the alarm.
B. Create an Amazon CloudWatch Logs metric filter and alarm for KMS events with an error message. Create an Amazon SNS topic as the target of the alarm. Subscribe the remediation Lambda function to the SNS topic.
C. Create an Amazon CloudWatch Events rule pattern looking for KMS service events with an error message. Create an Amazon SNS topic as the target of the rule. Subscribe the remediation Lambda function to the SNS topic.
D. Use Amazon CloudTrail to alert for KMS service events with an error message. Set the remediation Lambda function as the target of the rule.

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

**Explanation/Reference:**

**QUESTION 246**
A DevOps engineer is building a centralized CI/CD pipeline using AWS CodeBuild, AWS CodeDeploy, and Amazon S3. The engineer is required to have least privilege access and individual encryption at rest for all artifacts in Amazon S3. The engineer must be able to prune old artifacts without the ability to download or read them.



The engineer has already completed the following steps:
1. Created a unique AWS KMS CMK and S3 bucket for each project's builds.
2. Updated the S3 bucket policy to only allow uploads that use the associated KMS encryption.

Which final step should be taken to meet these requirements?

A. Update the attached IAM policies to allow access to the appropriate KMS key from the CodeDeploy role where the application will be deployed.
B. Update the attached IAM policies to allow access to the appropriate KMS key from the EC2 instance roles where the application will be deployed.
C. Update the CMK key policy to allow access to the appropriate KMS key from the CodeDeploy role where the application will be deployed.
D. Update the CMK key policy to allow to the appropriate KMS key from the EC2 instance roles where the application will be deployed.

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

**Explanation/Reference:**

**QUESTION 247**
A DevOps engineer is designing a multi-Region disaster recovery strategy for an application requiring an RPO of 1 hour and RTO of 4 hours. The application is deployed with an AWS CloudFormation template that creates an Application Load Balancer, Amazon EC2 instances in an Auto Scaling group, and an Amazon RDS Multi-AZ DB instance with 20 GB of allocated storage. The AMI of the application instance does not contain data and has been copied to the destination Region.
Which combination of actions will satisfy the recovery objectives at the LOWEST cost? (Choose two.)

A. Launch an RDS DB instance in the failover Region and use AWS DMS to configure ongoing replication from the source database.
B. Schedule an AWS Lambda function to take a snapshot of the database every hour and copy the snapshot to the failover Region.
C. Upon failover, update the CloudFormation stack in the failover Region to update the Auto Scaling group from one running instance to the desired number of instances. When the stack update is complete, change the DNS records to pointto the failover Region's Elastic Load Balancer.
D. Upon failover, launch the CloudFormation template in the failover Region with the snapshot ID as an input parameter. When the stack creation is complete, change the DNS records to point to the failover Region's Elastic Load Balancer.
E. Utilizing the build-in RDS automated backups, set up an event with Amazon CloudWatch Events that triggers an AWS Lambda function to copy the snapshot to the failover Region.

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

**Explanation/Reference:**



**QUESTION 248**
A company is adopting serverless computing and is migrating some of its existing applications to AWS Lambda. A DevOps engineer must come up with an automated deployment strategy using AWS CodePipeline that should include proper version controls, branching strategies, and rollback methods.
Which combination of steps should the DevOps engineer follow when setting up the pipeline? (Choose three.)

A. Use Amazon S3 as the source code repository.
B. Use AWS CodeCommit as the source code repository.
C. Use AWS CloudFormation to create an AWS Serverless Application Model (AWS SAM) template for deployment.
D. Use AWS CodeBuild to create an AWS Serverless Application Model (AWS SAM) template for deployment.
E. Use AWS CloudFormation to deploy the application.
F. Use AWS CodeDeploy to deploy the application.

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

**Explanation/Reference:**

**QUESTION 249**
After a data leakage incident that led to thousands of stolen user profiles, a compliance officer is demanding automatic, auditable security policy checks for all of the company's data stores, starting with public access of Amazon S3 buckets.
Which solution will accomplish this with the LEAST amount of effort?

A. Create a custom rule in AWS Config triggered by an S3 bucket configuration change that detects when the bucket policy or bucket ACL allows public read access. Use a remediation action to trigger an AWS Lambda function thatautomatically disables public access.
B. Create a custom rule in AWS Config triggered by an S3 bucket configuration change that detects when the bucket policy or bucket ACL allows public read access. Trigger an AWS Lambda function that automatically disables publicaccess.
C. Use a managed rule in AWS Config triggered by an S3 bucket configuration change that detects when the bucket policy or bucket ACL allows public read access. Configure a remediation action that automatically disables public access.
D. Use a managed rule in AWS Config triggered by an S3 bucket configuration change that detects when the bucket policy or bucket ACL allows public read access. Configure an AWS Lambda function that automatically disables publicaccess.

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



**Explanation/Reference:**
Reference: https://docs.aws.amazon.com/config/latest/developerguide/s3-bucket-public-read-prohibited.html

**QUESTION 250**
A company uses AWS KMS with CMKs and manual key rotation to meet regulatory compliance requirements. The security team wants to be notified when any keys have not been rotated after 90 days.
Which solution will accomplish this?

A. Configure AWS KMS to publish to an Amazon SNS topic when keys are more than 90 days old.
B. Configure an Amazon CloudWatch Events event to launch an AWS Lambda function to call the AWS Trusted Advisor API and publish to an Amazon SNS topic.
C. Develop an AWS Config custom rule that publishes to an Amazon SNS topic when keys are more than 90 days old.
D. Configure AWS Security Hub to publish to an Amazon SNS topic when keys are more than 90 days old.

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

**Explanation/Reference:**

**QUESTION 251**
A company develops and maintains a web application using Amazon EC2 instances and an Amazon RDS for SQL Server DB instance in a single Availability Zone. The resources need to run only when new deployments are being tested using AWS CodePipeline. Testing occurs one or more times a week and each test takes 2-3 hours to run. A DevOps engineer wants a solution that does not change the architecture components.
Which solution will meet these requirements in the MOST cost-effective manner?

A. Convert the RDS database to an Amazon Aurora Serverless database. Use an AWS Lambda function to start and stop the EC2 instances before and after tests.
B. Put the EC2 instances into an Auto Scaling group. Schedule scaling to run at the start of the deployment tests.
C. Replace the EC2 instances with EC2 Spot Instances and the RDS database with an RDS Reserved Instance.
D. Subscribe Amazon Cloud Watch Events to CodePipeline to trigger AWS Systems Manager Automation documents that start and stop all EC2 and RDS instances before and after deployment tests.

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



**Explanation/Reference:**
Reference: https://docs.amazonaws.cn/en_us/elasticbeanstalk/latest/dg/using-features.managing.as.html?filter-select=AWS%20Management%20Console

**QUESTION 252**
A company is using AWS CodePipeline to automate its release pipeline. AWS CodeDeploy is being used in the pipeline to deploy an application to Amazon ECS using the blue/green deployment model. The company wants to implement scripts to test the green version of the application before shifting traffic. These scripts will complete in 5 minutes or less. If errors are discovered during these tests, the application must be rolled back.
Which strategy will meet these requirements?

A. Add a stage to the CodePipeline pipeline between the source and deploy stages. Use AWS CodeBuild to create an execution environment and build commands in the buildspec file to invoke test scripts. If errors are found, use the awsdeploy stop-deployment command to stop the deployment.
B. Add a stage to the CodePipeline pipeline between the source and deploy stages. Use this stage to execute an AWS Lambda function that will run the test scripts. If errors are found, use the aws deploy stop-deployment command to stopthe deployment.
C. Add a hooks section to the CodeDeploy AppSpec file. Use the AfterAllowTestTraffic lifecycle event to invoke an AWS Lambda function to run the test scripts. If errors are found, exit the Lambda function with an error to trigger rollback.
D. Add a hooks section to the CodeDeploy AppSpec file. Use the AfterAllowTraffic lifecycle event to invoke the test scripts. If errors are found, use the aws deploy stop-deployment CLI command to stop the deployment.

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

**Explanation/Reference:**
Section: (none)

Reference: https://docs.aws.amazon.com/codedeploy/latest/userguide/reference-appspec-file-structure-hooks.html

**QUESTION 253**
A company has 100 GB of log data in an Amazon S3 bucket stored in .csv format. SQL developers want to query this data and generate graphs to visualize it. They also need an efficient, automated way to store metadata from the .csv file. Which combination of steps should be taken to meet these requirements with the LEAST amount of effort? (Choose three.)

A. Filter the data through AWS X-Ray to visualize the data.
B. Filter the data through Amazon QuickSight to visualize the data.
C. Query the data with Amazon Athena.
D. Query the data with Amazon Redshift.
E. Use AWS Glue as the persistent metadata store.
F. Use Amazon S3 as the persistent metadata store.



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

**Explanation/Reference:**

**QUESTION 254**
A company is using AWS CodePipeline to deploy an application. A recent policy change requires that a member of the company's security team sign off on any application changes before they are deployed into production. The approval should be recorded and retained.
Which combination of actions will meet these new requirements? (Choose two.)

A. Configure CodePipeline with Amazon CloudWatch Logs to retain data.
B. Configure CodePipeline to deliver action logs to Amazon S3.
C. Create an AWS CloudTrail trail to deliver logs to Amazon S3.
D. Create a custom CodePipeline action to invoke an AWS Lambda function for approval. Create a policy that gives the security team access to manage custom CodePipeline actions.

E. Create a manual approval CodePipeline action before the deployment step. Create a policy that grants the security team access to approve manual approval stages.

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

**Explanation/Reference:**

**QUESTION 255**
An application's users are encountering bugs immediately after Amazon API Gateway deployments. The development team deploys once or twice a day and uses a blue/green deployment strategy with custom health checks and automated rollbacks. The team wants to limit the number of users affected by deployment bugs and receive notifications when rollbacks are needed.
Which combination of steps should a DevOps engineer use to meet these requests? (Choose two.)

A. Implement a blue/green strategy using path mappings.
B. Implement a canary deployment strategy.
C. Implement a rolling deployment strategy using multiple stages.
D. Use Amazon CloudWatch alarms to notify the development team.
E. Use Amazon CloudWatch Events to notify the development team.



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

**Explanation/Reference:**

**QUESTION 256**
A DevOps engineer has been tasked with ensuring that all Amazon S3 buckets, except for those with the word "public" in the name, allow access only to authorized users utilizing S3 bucket policies. The security team wants to be notified when a bucket is created without the proper policy and for the policy to be automatically updated.
Which solutions will meet these requirements?

A. Create a custom AWS Config rule that will trigger an AWS Lambda function when an S3 bucket is created or updated. Use the Lambda function to look for S3 buckets that should be private, but that do not have a bucket policy thatenforces privacy. When such a bucket is found, invoke a remediation action and use Amazon SNS to notify the security team.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that triggers when an S3 bucket is created. Use an AWS Lambda function to determine

whether the bucket should be private. If the bucket should be private, update thePublicAccessBlock configuration. Configure a second EventBridge (CloudWatch Events) rule to notify the security team using Amazon SNS when PutBucketPolicy is called.

C. Create an Amazon S3 event notification that triggers when an S3 bucket is created that does not have the word "public" in the name. Define an AWS Lambda function as a target for this notification and use the function to apply a newdefault policy to the S3 bucket. Create an additional notification with the same filter and use Amazon SNS to send an email to the security team.

D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that triggers when a new object is created in a bucket that does not have the word "public" in the name. Target and use an AWS Lambda function to update thePublicAccessBlock configuration. Create an additional notification with the same filter and use Amazon SNS to send an email to the security team.

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

**Explanation/Reference:**

**QUESTION 257**
A company is using AWS to deploy an application. The development team must automate the deployments. The team has created an AWS CodePipeline pipeline to deploy the application to Amazon EC2 instances using AWS CodeDeploy after it has been built using AWS CodeBuild.
The team wants to add automated testing to the pipeline to confirm that the application is healthy before deploying the code to the EC2 instances. The team also requires a manual approval action before the application is deployed, even if the tests are successful. The testing and approval must be accomplished at the lowest costs, using the simplest management solution.
Which solution will meet these requirements?



A. Create a manual approval action after the build action of the pipeline. Use Amazon SNS to inform the team of the stage being triggered. Next, add a test action using CodeBuild to perform the required tests. At the end of the pipeline,add a deploy action to deploy the application to the next stage.

B. Create a test action after the CodeBuild build of the pipeline. Configure the action to use CodeBuild to perform the required test. If these tests are successful, mark the action as successful. Add a manual approval action that usesAmazon SNS to notify the team, and add a deploy action to deploy the application to the next stage.

C. Create a new pipeline that uses a source action that gets the code from the same repository as the first pipeline. Add a deploy action to deploy the code to a test environment. Use a test action using AWS Lambda to test the deployment.Add a manual approval action by using Amazon SNS to notify the team, and add a deploy action to deploy the application to the next stage.

D. Create a test action after the build action. Use a Jenkins server on Amazon EC2 to perform the required tests and mark the action as successful if the tests pass. Create a manual approval action that uses Amazon SQS to notify the teamand add a deploy action to deploy the application to the next stage.

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

**Explanation/Reference:**

**QUESTION 258**
A company is developing a web application's infrastructure using AWS CloudFormation. The database engineering team maintains the database resources in a CloudFormation template, and the software development team maintains the web application resources in a separate CloudFormation template. As the scope of the application grows, the software development team needs to use resources maintained by the database engineering team. However, both teams have their own review and lifecycle management processes that they want to keep. Both teams also require resource-level change-set reviews. The software development team would like to deploy changes to this template using their CI/CD pipeline.
Which solution will meet these requirements?

A. Create a stack export from the database CloudFormation template and import those references into the web application CloudFormation template.
B. Create a CloudFormation nested stack to make cross-stack resource references and parameters available in both stacks.
C. Create a CloudFormation stack set to make cross-stack resource references and parameters available in both stacks.
D. Create input parameters in the web application CloudFormation template and pass resource names and IDs from the database stack.

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

**Explanation/Reference:**



**QUESTION 259**
An ecommerce company is receiving reports that its order history page is experiencing delays in reflecting the processing status of orders. The order processing system consists of an AWS Lambda function using reserved concurrency. The Lambda function processes order messages from an Amazon SQS queue and inserts processed orders into an Amazon DynamoDB table. The DynamoDB table has Auto Scaling enabled for read and write capacity. Which actions will diagnose and resolve the delay? (Choose two.)

A. Check the ApproximateAgeOfOldestMessage metric for the SQS queue and increase the Lambda function concurrency limit.
B. Check the ApproximateAgeOfOldestMessage metric for the SQS queue and configure a redrive policy on the SQS queue.
C. Check the NumberOfMessagesSent metric for the SQS queue and increase the SQS queue visibility timeout.
D. Check the ThrottledWriteRequests metric for the DynamoDB table and increase the maximum write capacity units for the table's Auto Scaling policy.
E. Check the Throttles metric for the Lambda function and increase the Lambda function timeout.

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

**Explanation/Reference:**

**QUESTION 260**
A DevOps engineer is implementing governance controls for a company that requires its infrastructure to be housed within the United States. The engineer must restrict which Regions can be used, and ensure an alert is sent as soon as possible if any activity outside the governance policy takes place. The controls should be automatically enabled on any new Region outside the United States.
Which combination of actions will meet these requirements? (Choose two.)

A. Create an AWS Organizations SCP that denies access to all non-global services in non-US Regions. Attach the policy to the root of the organization.
B. Configure AWS CloudTrail to send logs to Amazon CloudWatch Logs and enable it for all Regions. Use a CloudWatch Logs metric filter to send an alert on any service activity in non-US Regions.
C. Use an AWS Lambda function that checks for AWS service activity and deploy it to all Regions. Write an Amazon CloudWatch Events rule that runs the Lambda function every hour, sending an alert if activity is found in a non-USRegion.
D. Use an AWS Lambda function to query Amazon Inspector to look for service activity in non-US Regions and send alerts if any activity is found.
E. Write an SCP using the aws:RequestedRegion condition key limiting access to US Regions. Apply the policy to all users, groups, and roles.

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

**Explanation/Reference:**



**QUESTION 261**
Due to compliance regulations, management has asked you to provide a system that allows for cost-effective long-term storage of your application logs and provides a way for support staff to view the logs more quickly. Currently your log system archives logs automatically to Amazon S3 every hour, and support staff must wait for these logs to appear in Amazon S3, because they do not currently have access to the systems to view live logs.
What method should you use to become compliant while also providing a faster way for support staff to have access to logs?

A. Update Amazon S3 lifecycle policies to archive old logs to Amazon Glacier, and add a new policy to push all log entries to Amazon SQS for ingestion by the support team
B. Update Amazon S3 lifecycle policies to archive old logs to Amazon Glacier, and use or write a service to also stream your application logs to CloudWatch Logs.
C. Update Amazon Glacier lifecycle policies to pull new logs from Amazon S3, and in the Amazon EC2 console, enable the CloudWatch Logs Agent on all of your application servers.
D. Update Amazon S3 lifecycle policies to archive old logs to Amazon Glacier. key can be different from the tableEnable Amazon S3 partial uploads on your Amazon S3 bucket, and trigger an Amazon SNS notification when a partial uploadoccurs.
E. Use or write a service to stream your application logs to CloudWatch Logs. Use an Amazon Elastic Map Reduce cluster to live stream your logs from CloudWatch Logs for ingestion by the support team, and create a Hadoop job to pushthe logs to S3 in five-minute chunks.

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

**Explanation/Reference:**

**QUESTION 262**
You want to securely distribute credentials for your Amazon RDS instance to your fleet of web server instances. The credentials are stored in a file that is controlled by a configuration management system. How do you securely deploy the credentials in an automated manner across the fleet of web server instances, which can number in the hundreds, while retaining the ability to roll back if needed?

A. Store your credential files in an Amazon S3 bucket. Use Amazon S3 server-side encryption on the credential files. Have a scheduled job that pulls down the credential files into the instances every 10 minutes.
B. Store the credential files in your version-controlled repository with the rest of your code. Have a post-commit action in version control that kicks off a job in your continuous integration system which securely copses the new credential filesto all web server instances.
C. Insert credential files into user data and use an instance lifecycle policy to periodically refresh the file from the user data.
D. Keep credential files as a binary blob in an Amazon RDS MySQL DB instance, and have a script on each Amazon EC2 instance that pulls the files down from the RDS instance.
E. Store the credential files in your version-controlled repository with the rest of your code. Use a parallel file copy program to send the credential files from your local machine to the Amazon EC2 instances.



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

**Explanation/Reference:**

**QUESTION 263**
You are using a configuration management system to manage your Amazon EC2 instances. On your Amazon EC2 Instances, you want to store credentials for connecting to an Amazon RDS DB instance. How should you securely store these credentials?

A. Give the Amazon EC2 instances an IAM role that allows read access to a private Amazon S3 bucket. Store a file with database credentials in the Amazon S3 bucket. Have your configuration management system pull the file from thebucket when it is needed.
B. Launch an Amazon EC2 instance and use the configuration management system to bootstrap the instance with the Amazon RDS DB credentials. Create an AMI from this instance.
C. Store the Amazon RDS DB credentials in Amazon EC2 user data. Import the credentials into the Instance on boot.

D. Assign an IAM role to your Amazon RDS instance, and use this IAM role to access the Amazon RDS DB from your Amazon EC2 instances.
E. Store your credentials in your version control system, in plaintext. Check out a copy of your credentials from the version control system on boot. Use Amazon EBS encryption on the volume storing the Amazon RDS DB credentials.

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

**Explanation/Reference:**

**QUESTION 264**
Your company has developed a web application and is hosting it in an Amazon S3 bucket configured for static website hosting. The application is using the AWS SDK for JavaScript in the browser to access data stored in an Amazon DynamoDB table.
How can you ensure that API keys for access to your data in DynamoDB are kept secure?

A. Create an Amazon S3 role in IAM with access to the specific DynamoDB tables, and assign it to the bucket hosting your website.
B. Configure S3 bucket tags with your AWS access keys for your bucket hosing your website so that the application can query them for access.
C. Configure a web identity federation role within IAM to enable access to the correct DynamoDB resources and retrieve temporary credentials.
D. Store AWS keys in global variables within your application and configure the application to use these credentials when making requests.



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

**Explanation/Reference:**

**QUESTION 265**
You need to implement A/B deployments for several multi-tier web applications. Each of them has its Individual infrastructure: Amazon Elastic Compute Cloud (EC2) front-end servers, Amazon ElastiCache clusters, Amazon Simple Queue Service (SQS) queues, and Amazon Relational Database (RDS) Instances.
Which combination of services would give you the ability to control traffic between different deployed versions of your application?

A. Create one AWS Elastic Beanstalk application and all AWS resources (using configuration files inside the application source bundle) for each web application. New versions would be deployed a-eating Elastic Beanstalk environmentsand using the Swap URLs feature.
B. Using AWS CloudFormation templates, create one Elastic Beanstalk application and all AWS resources (in the same template) for each web application. New versions would be deployed using AWS CloudFormation templates to createnew Elastic Beanstalk environments, and traffic would be balanced between them using weighted Round Robin (WRR) records in Amazon Route53.
C. Using AWS CloudFormation templates, create one Elastic Beanstalk application and all AWS resources (in the same template) for each web application. New

versions would be deployed updating a parameter on the CloudFormationtemplate and passing it to the cfn-hup helper daemon, and traffic would be balanced between them using Weighted Round Robin (WRR) records in Amazon Route 53.

D. Create one Elastic Beanstalk application and all AWS resources (using configuration files inside the application source bundle) for each web application. New versions would be deployed updating the Elastic Beanstalk application versionfor the current Elastic Beanstalk environment.

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

**Explanation/Reference:**

**QUESTION 266**
You work for an insurance company and are responsible for the day-to-day operations of your company's online quote system used to provide insurance quotes to members of the public. Your company wants to use the application logs generated by the system to better understand customer behavior. Industry, regulations also require that you retain all application logs for the system indefinitely in order to investigate fraudulent claims in the future. You have been tasked with designing a log management system with the following requirements:
- All log entries must be retained by the system, even during unplanned instance failure.
- The customer insight team requires immediate access to the logs from the past seven days.
- The fraud investigation team requires access to all historic logs, but will wait up to 24 hours before these logs are available.
How would you meet these requirements in a cost-effective manner? (Choose three.)



A. Configure your application to write logs to the instance's ephemeral disk, because this storage is free and has good write performance. Create a script that moves the logs from the instance to Amazon 53 once an hour.

B. Write a script that is configured to be executed when the instance is stopped or terminated and that will upload any remaining logs on the instance to Amazon S3.

C. Create an Amazon S3 lifecycle configuration to move log files from Amazon S3 to Amazon Glacier after seven days.

D. Configure your application to write logs to the instance's default Amazon EBS boot volume, because this storage already exists. Create a script that moves the logs from the instance to Amazon 53 once an hour.

E. Configure your application to write logs to a separate Amazon EBS volume with the "delete on termination" field set to false. Create a script that moves the logs from the instance to Amazon S3 once an hour.

F. Create a housekeeping script that runs on a T2 micro instance managed by an Auto Scaling group for high availability. The script uses the AWS API to identify any unattached Amazon EBS volumes containing log files. Yourhousekeeping script will mount the Amazon EBS volume, upload all logs to Amazon S3, and then delete the volume.

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

**Explanation/Reference:**

**QUESTION 267**
You have an application running on Amazon EC2 in an Auto Scaling group. Instances are being bootstrapped dynamically, and the bootstrapping takes over 15 minutes to complete. You find that instances are reported by Auto Scaling as being In Service before bootstrapping has completed. You are receiving application alarms related to new instances before they have completed bootstrapping, which is causing confusion. You find the cause: your application monitoring tool is polling the Auto Scaling Service API for instances that are In Service, and creating alarms for new previously unknown instances. Which of the following will ensure that new instances are not added to your application monitoring tool before bootstrapping is completed?

A. Create an Auto Scaling group lifecycle hook to hold the instance in a pending: wait state until your bootstrapping is complete. Once bootstrapping is complete, notify Auto Scaling to complete the lifecycle hook and move the instance intoa pending: complete state.
B. Use the default Amazon CloudWatch application metrics to monitor your application's health. Configure an Amazon SNS topic to send these CloudWatch alarms to the correct recipients.
C. Tag all instances on launch to identify that they are in a pending state. Change your application monitoring tool to look for this tag before adding new instances, and the use the Amazon API to set the instance state to 'pending' untilbootstrapping is complete.
D. Increase the desired number of instances in your Auto Scaling group configuration to reduce the time it takes to bootstrap future instances.

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



**Explanation/Reference:**

**QUESTION 268**
You have been given a business requirement to retain log files for your application for 10 years. You need to regularly retrieve the most recent logs for troubleshooting. Your logging system must be cost-effective, given the large volume of logs.
What technique should you use to meet these requirements?

A. Store your log in Amazon CloudWatch Logs.
B. Store your logs in Amazon Glacier.
C. Store your logs in Amazon S3, and use lifecycle policies to archive to Amazon Glacier.
D. Store your logs in HDFS on an Amazon EMR cluster.
E. Store your logs on Amazon EBS, and use Amazon EBS snapshots to archive them.

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

**Explanation/Reference:**

**QUESTION 269**
You work for a startup that has developed a new photo-sharing application for mobile devices. Over recent months, your application has increased in popularity; this has resulted in a decrease in the performance of the application clue to the increased load. Your application has a two-tier architecture that is composed of an Auto Scaling PHP application tier and a MySQL RDS instance initially deployed with AWS CloudFormation. Your Auto Scaling group has a min value of 4 and a max value of 8. The desired capacity is now at 8 because of the high CPU utilization of the instances. After some analysis, you are confident that the performance issues stem from a constraint in CPU capacity, although memory utilization remains low. You therefore decide to move from the general-purpose M3 instances to the compute-optimized C3 instances. How would you deploy this change while minimizing any interruption to your end users?

A. Sign into the AWS Management Console, copy the old launch configuration, and create a new launch configuration that specifies the C3 instances. Update the Auto Scaling group with the new launch configuration. Auto Scaling will thenupdate the instance type of all running instances.
B. Sign into the AWS Management Console, and update the existing launch configuration with the new C3 instance type. Add an UpdatePolicy attribute to your Auto Scaling group that specifies AutoScalingRollingUpdate.
C. Update the launch configuration specified in the AWS CloudFormation template with the new C3 instance type. Run a stack update with the new template. Auto Scaling will then update the instances with the new instance type.
D. Update the launch configuration specified in the AWS CloudFormation template with the new C3 instance type. Also add an UpdatePolicy attribute to your Auto Scaling group that specifies AutoScalingRollingUpdate. Run a stack updatewith the new template.



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

**Explanation/Reference:**

**QUESTION 270**
You have been tasked with implementing an automated data backup solution for your application servers that run on Amazon EC2 with Amazon EBS volumes. You want to use a distributed data store for your backups to avoid single points of failure and to increase the durability of the data. Daily backups should be retained for 30 days so that you can restore data within an hour. How can you implement this through a script that a scheduling daemon runs daily on the application servers?

A. Write the script to call the ec2-create-volume API, tag the Amazon EBS volume with the current date time group, and copy backup data to a second Amazon EBS volume. Use the ec2-describe-volumes API to enumerate existing backupvolumes. Call the ec2-delete-volume API to prune backup volumes that are tagged with a date-tine group older than 30 days.
B. Write the script to call the Amazon Glacier upload archive API, and tag the backup archive with the current date-time group. Use the list vaults API to enumerate existing backup archives Call the delete vault API to prune backuparchives that are tagged with a date-time group older than 30 days.
C. Write the script to call the ec2-create-snapshot API, and tag the Amazon EBS snapshot with the current date-time group. Use the ec2-describe-snapshot API

to enumerate existing Amazon EBS snapshots. Call the ec2-delete-snapShotAPI to prune Amazon EBS snapshots that are tagged with a datetime group older than 30 days.

D. Write the script to call the ec2-create-volume API, tag the Amazon EBS volume with the current date-time group, and use the ec2-copy-snapshot API to back up data to the new Amazon EBS volume. Use the ec2- describe-snapshot APIto enumerate existing backup volumes. Call the ec2-delete-snaphot API to prune backup Amazon EBS volumes that are tagged with a date-time group older than 30 days.

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

**Explanation/Reference:**

**QUESTION 271**
Your application uses CloudFormation to orchestrate your application's resources. During your testing phase before the application went live, your Amazon RDS instance type was changed and caused the instance to be re-created, resulting In the loss of test data.
How should you prevent this from occurring in the future?

A. Within the AWS CloudFormation parameter with which users can select the Amazon RDS instance type, set AllowedValues to only contain the current instance type.

B. Use an AWS CloudFormation stack policy to deny updates to the instance. Only allow UpdateStack permission to IAM principals that are denied SetStackPolicy.

C. In the AWS CloudFormation template, set the AWS::RDS::DBInstance's DBInstanceClass property to be read-only.

D. Subscribe to the AWS CloudFormation notification "BeforeResourceUpdate," and call CancelStackUpdate if the resource identified is the Amazon RDS instance.

E. In the AWS CloudFormation template, set the DeletionPolicy of the AWS::RDS::DBInstance's DeletionPolicy property to "Retain."

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

**Explanation/Reference:**

**QUESTION 272**
Your company develops a variety of web applications using many platforms and programming languages with different application dependencies. Each application must be developed and deployed quickly and be highly evadable to satisfy your business requirements.
Which of the following methods should you use to deploy these applications rapidly?

A. Develop the applications in Docker containers, and then deploy them to Elastic Beanstalk environments with Auto Scaling and Elastic Load Balancing.
B. Use the AWS CloudFormation Docker import service to build and deploy the applications with high availability in multiple Availability Zones.
C. Develop each application's code in DynamoDB, and then use hooks to deploy it to Elastic Beanstalk environments with Auto Scaling and Elastic Load Balancing.
D. Store each application's code in a Git repository, develop custom package repository managers for each application's dependencies, and deploy to AWS OpsWorks in multiple Availability Zones.

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

**Explanation/Reference:**

**QUESTION 273**
You have a large number of web servers in an Auto Scaling group behind a load balancer. On an hourly basis, you want to filter and process the logs to collect data on unique visitors, and then put that data in a durable data store in order to run reports. Web servers in the Auto Scaling group are constantly launching and terminating based on your scaling policies, but you do not want to lose any of the log data from these servers during a stop/termination initiated by a user or by Auto Scaling.
What two approaches will meet these requirements? (Choose two.)



A. Install an Amazon Cloudwatch Logs Agent on every web server during the bootstrap process. Create a CloudWatch log group and define Metric Filters to create custom metrics that track unique visitors from the streaming web serverlogs. Create a scheduled task on an Amazon EC2 instance that runs every hour to generate a new report based on the Cloudwatch custom metrics.
B. On the web servers, create a scheduled task that executes a script to rotate and transmit the logs to Amazon Glacier. Ensure that the operating system shutdown procedure triggers a logs transmission when the Amazon EC2 instance isstopped/terminated. Use Amazon Data Pipeline to process the data in Amazon Glacier and run reports every hour.
C. On the web servers, create a scheduled task that executes a script to rotate and transmit the logs to an Amazon S3 bucket. Ensure that the operating system shutdown procedure triggers a logs transmission when the Amazon EC2instance is stopped/terminated. Use AWS Data Pipeline to move log data from the Amazon S3 bucket to Amazon Redshift In order to process and run reports every hour.
D. Install an AWS Data Pipeline Logs Agent on every web server during the bootstrap process. Create a log group object in AWS Data Pipeline, and define Metric Filters to move processed log data directly from the web servers to AmazonRedshift and run reports every hour.

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

**Explanation/Reference:**

**QUESTION 274**
You have been tasked with deploying a scalable distributed system using AWS OpsWorks. Your distributed system is required to scale on demand. As it is distributed, each node must hold a configuration file that includes the hostnames of the other instances within the layer.
How should you configure AWS OpsWorks to manage scaling this application dynamically?

A. Create a Chef Recipe to update this configuration file, configure your AWS OpsWorks stack to use custom cookbooks, and assign this recipe to the Configure LifeCycle Event of the specific layer.
B. Update this configuration file by writing a script to poll the AWS OpsWorks service API for new instances. Configure your base AMI to execute this script on Operating System startup.
C. Create a Chef Recipe to update this configuration file, configure your AWS OpsWorks stack to use custom cookbooks, and assign this recipe to execute when instances are launched.
D. Configure your AWS OpsWorks layer to use the AWS-provided recipe for distributed host configuration, and configure the instance hostname and file path parameters in your recipes settings.

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

**Explanation/Reference:**



**QUESTION 275**
You have an application running on an Amazon EC2 instance and you are using IAM roles to securely access AWS Service APIs. How can you configure your application running on that instance to retrieve the API keys for use with the AWS SDKs?

A. When assigning an EC2 IAM role to your instance in the console, in the "Chosen SDK" dropdown list, select the SDK that you are using, and the instance will configure the correct SDK on launch with the API keys.
B. Within your application code, make a GET request to the IAM Service API to retrieve credentials for your user.
C. When using AWS SDKs and Amazon EC2 roles, you do not have to explicitly retrieve API keys, because the SDK handles retrieving them from the Amazon EC2 MetaData service.
D. Within your application code, configure the AWS SDK to get the API keys from environment variables, because assigning an Amazon EC2 role stores keys in environment variables on launch.

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

**Explanation/Reference:**

**QUESTION 276**
When an Auto Scaling group is running in Amazon Elastic Compute Cloud (EC2), your application rapidly scales up and down in response to load within a 10-minute window; however, after the load peaks, you begin to see problems in your configuration management system where previously terminated Amazon EC2 resources are still showing as active. What would be a reliable and efficient way to handle the cleanup of Amazon EC2 resources within your configuration management system? (Choose two.)

A. Write a script that is run by a daily cron job on an Amazon EC2 instance and that executes API Describe calls of the EC2 Auto Scaling group and removes terminated instances from the configuration management system.
B. Configure an Amazon Simple Queue Service (SQS) queue for Auto Scaling actions that has a script that listens for new messages and removes terminated instances from the configuration management system.
C. Use your existing configuration management system to control the launching and bootstrapping of instances to reduce the number of moving parts in the automation.
D. Write a small script that is run during Amazon EC2 instance shutdown to de-register the resource from the configuration management system.
E. Use Amazon Simple Workflow Service (SWF) to maintain an Amazon DynamoDB database that contains a whitelist of instances that have been previously launched, and allow the Amazon SWF worker to remove information from theconfiguration management system.

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



**Explanation/Reference:**

**QUESTION 277**
You have enabled Elastic Load Balancing HTTP health checking. After looking at the AWS Management Console, you see that all instances are passing health checks, but your customers are reporting that your site is not responding. What is the cause?

A. The HTTP health checking system is misreporting due to latency in inter-instance metadata synchronization.
B. The health check in place is not sufficiently evaluating the application function.
C. The application is returning a positive health check too quickly for the AWS Management Console to respond.
D. Latency in DNS resolution is interfering with Amazon EC2 metadata retrieval.

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

**Explanation/Reference:**

**QUESTION 278**
You use Amazon CloudWatch as your primary monitoring system for your web application. After a recent software deployment, your users are getting Intermittent 500 Internal Server Errors when using the web application. You want to create a CloudWatch alarm, and notify an on-call engineer when these occur. How can you accomplish this using AWS services? (Choose three.)

A. Deploy your web application as an AWS Elastic Beanstalk application. Use the default Elastic Beanstalk Cloudwatch metrics to capture 500 Internal Server Errors. Set a CloudWatch alarm on that metric.
B. Install a CloudWatch Logs Agent on your servers to stream web application logs to CloudWatch.
C. Use Amazon Simple Email Service to notify an on-call engineer when a CloudWatch alarm is triggered.
D. Create a CloudWatch Logs group and define metric filters that capture 500 Internal Server Errors. Set a CloudWatch alarm on that metric.
E. Use Amazon Simple Notification Service to notify an on-call engineer when a CloudWatch alarm is triggered.
F. Use AWS Data Pipeline to stream web application logs from your servers to CloudWatch.

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

**Explanation/Reference:**



**QUESTION 279**
After a daily scrum with your development teams, you've agreed that using Blue/Green style deployments would benefit the team. Which technique should you use to deliver this new requirement?

A. Re-deploy your application on AWS Elastic Beanstalk, and take advantage of Elastic Beanstalk deployment types.
B. Using an AWS CloudFormation template, re-deploy your application behind a load balancer, launch a new AWS CloudFormation stack during each deployment, update your load balancer to send half your traffic to the new stack whileyou test, after verification update the load balancer to send 100% of traffic to the new stack, and then terminate the old stack.
C. Re-deploy your application behind a load balancer that uses Auto Scaling groups, create a new identical Auto Scaling group, and associate it to the load balancer. During deployment, set the desired number of instances on the old AutoScaling group to zero, and when all instances have terminated, delete the old Auto Scaling group.
D. Using an AWS OpsWorks stack, re-deploy your application behind an Elastic Load Balancing load balancer and take advantage of OpsWorks stack versioning, during deployment create a new version of your application, tell OpsWorksto launch the new version behind your load balancer, and when the new version is launched, terminate the old OpsWorks stack.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 280**
Your development team wants account-level access to production instances in order to do live debugging of a highly secure environment. Which of the following should you do?

A. Place the credentials provided by Amazon Elastic Compute Cloud (EC2) into a secure Amazon Sample Storage Service (S3) bucket with encryption enabled. Assign AWS Identity and Access Management (IAM) users to each developerso they can download the credentials file.
B. Place an internally created private key into a secure S3 bucket with server-side encryption using customer keys and configuration management, create a service account on all the instances using this private key, and assign IAM users toeach developer so they can download the file.
C. Place each developer's own public key into a private S3 bucket, use instance profiles and configuration management to create a user account for each developer on all instances, and place the user's public keys into the appropriateaccount.
D. Place the credentials provided by Amazon EC2 onto an MFA encrypted USB drive, and physically share it with each developer so that the private key never leaves the office.

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



**Explanation/Reference:**

**QUESTION 281**
As part of your continuous deployment process, your application undergoes an I/O load performance test before it is deployed to production using new AMIs. The application uses one Amazon Elastic Block Store (EBS) PIOPS volume per instance and requires consistent I/O performance.
Which of the following must be carried out to ensure that I/O load performance tests yield the correct results in a repeatable manner?

A. Ensure that the I/O block sizes for the test are randomly selected.
B. Ensure that the Amazon EBS volumes have been pre-warmed by reading all the blocks before the test.
C. Ensure that snapshots of the Amazon EBS volumes are created as a backup.
D. Ensure that the Amazon EBS volume is encrypted.
E. Ensure that the Amazon EBS volume has been pre-warmed by creating a snapshot of the volume before the test.

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

**Explanation/Reference:**

**QUESTION 282**
After reviewing the last quarter's monthly bills, management has noticed an increase in the overall bill from Amazon. After researching this increase in cost, you discovered that one of your new services is doing a lot of GET Bucket API calls to Amazon S3 to build a metadata cache of all objects in the applications bucket. Your boss has asked you to come up with a new cost-effective way to help reduce the amount of these new GET Bucket API calls. What process should you use to help mitigate the cost?

A. Update your Amazon S3 buckets' lifecycle policies to automatically push a list of objects to a new bucket, and use this list to view objects associated with the application's bucket.
B. Create a new DynamoDB table. Use the new DynamoDB table to store all metadata about all objects uploaded to Amazon S3. Any time a new object is uploaded, update the application's internal Amazon S3 object metadata cache fromDynamoDB.
C. Using Amazon SNS, create a notification on any new Amazon S3 objects that automatically updates a new DynamoDB table to store all metadata about the new object. Subscribe the application to the Amazon SNS topic to update itsinternal Amazon S3 object metadata cache from the DynamoDB table.
D. Upload all images to Amazon SQS, set up SQS lifecycles to move all images to Amazon S3, and initiate an Amazon SNS notification to your application to update the application's Internal Amazon S3 object metadata cache.
E. Upload all images to an ElastiCache filecache server. Update your application to now read all file metadata from the ElastiCache filecache server, and configure the ElastiCache policies to push all files to Amazon S3 for long-termstorage.



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

**Explanation/Reference:**

**QUESTION 283**
Your current log analysis application takes more than four hours to generate a report of the top 10 users of your web application. You have been asked to implement a system that can report this information in real time, ensure that the report is always up to date, and handle increases in the number of requests to your web application. Choose the option that is cost-effective and can fulfill the requirements.

A. Publish your data to CloudWatch Logs, and configure your application to autoscale to handle the load on demand.
B. Publish your log data to an Amazon S3 bucket. Use AWS CloudFormation to create an Auto Scaling group to scale your post-processing application which is configured to pull down your log files stored an Amazon S3.
C. Post your log data to an Amazon Kinesis data stream, and subscribe your log-processing application so that is configured to process your logging data.
D. Configure an Auto Scaling group to increase the size of your Amazon EMR duster.
E. Create a multi-AZ Amazon RDS MySQL cluster, post the logging data to MySQL, and run a map reduce job to retrieve the required information on user

counts.

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

**Explanation/Reference:**

**QUESTION 284**
You are using Elastic Beanstalk to manage your e-commerce store. The store is based on an open source e- commerce platform and is deployed across multiple instances in an Auto Scaling group. Your development team often creates new "extensions" for the e-commerce store. These extensions include PHP source code as well as an SQL upgrade script used to make any necessary updates to the database schema. You have noticed that some extension deployments fail due to an error when running the SQL upgrade script. After further investigation, you realize that this is because the SQL script is being executed on all of your Amazon EC2 instances.
How would you ensure that the SQL script is only executed once per deployment regardless of how many Amazon EC2 instances are running at the time?

A. Use a "Container command" within an Elastic Beanstalk configuration file to execute the script, ensuring that the "leader only" flag is set to true.
B. Make use of the Amazon EC2 metadata service to query whether the instance is marked as the leader" in the Auto Scaling group. Only execute the script if "true" is returned.
C. Use a "Solo Command" within an Elastic Beanstalk configuration file to execute the script. The Elastic Beanstalk service will ensure that the command is only executed once.
D. Update the Amazon RDS security group to only allow write access from a single instance in the Auto Scaling group; that way, only one instance will successfully execute the script on the database.

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

**Explanation/Reference:**

**QUESTION 285**
You are administering a continuous integration application that polls version control for changes and then launches new Amazon EC2 instances for a full suite of build tests. What should you do to ensure the lowest overall cost while being able to run as many tests in parallel as possible?

A. Perform syntax checking on the continuous integration system before launching a new Amazon EC2 instance for build test, unit and integration tests.
B. Perform syntax and build tests on the continuous integration system before launching the new Amazon EC2 instance unit and integration tests.
C. Perform all tests on the continuous integration system, using AWS OpsWorks for unit, integration, and build tests.

D. Perform syntax checking on the continuous integration system before launching a new AWS Data Pipeline for coordinating the output of unit, integration, and build tests.

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

**Explanation/Reference:**

**QUESTION 286**
You are doing a load testing exercise on your application hosted on AWS. While testing your Amazon RDS MySQL DB instance, you notice that when you hit 100% CPU utilization on it, your application becomes non- responsive. Your application is read-heavy.
What are methods to scale your data tier to meet the application's needs? (Choose three.)

A. Add Amazon RDS DB read replicas, and have your application direct read queries to them.
B. Add your Amazon RDS DB instance to an Auto Scaling group and configure your CloudWatch metric based on CPU utilization.
C. Use an Amazon SQS queue to throttle data going to the Amazon RDS DB instance.
D. Use ElastiCache in front of your Amazon RDS DB to cache common queries.
E. Shard your data set among multiple Amazon RDS DB instances.
F. Enable Multi-AZ for your Amazon RDS DB instance.



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

**Explanation/Reference:**

**QUESTION 287**
Your mobile application includes a photo-sharing service that is expecting tens of thousands of users at launch. You will leverage Amazon Simple Storage Service (S3) for storage of the user Images, and you must decide how to authenticate and authorize your users for access to these images. You also need to manage the storage of these images. Which two of the following approaches should you use? (Choose two.)

A. Create an Amazon S3 bucket per user, and use your application to generate the S3 URI for the appropriate content.
B. Use AWS Identity and Access Management (IAM) user accounts as your application-level user database, and offload the burden of authentication from your application code.
C. Authenticate your users at the application level, and use AWS Security Token Service (STS) to grant token-based authorization to S3 objects.
D. Authenticate your users at the application level, and send an SMS token message to the user. Create an Amazon S3 bucket with the same name as the SMS

message token, and move the user's objects to that bucket.

E. Use a key-based naming scheme comprised from the user IDs for all user objects in a single Amazon S3 bucket.

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

**Explanation/Reference:**

**QUESTION 288**
You have an Auto Sealing group of Instances that processes messages from an Amazon Simple Queue Service (SQS) queue. The group scales on the size of the queue. Processing Involves calling a third-party web service. The web service is complaining about the number of failed and repeated calls it is receiving from you. You have noticed that when the group scales in, instances are being terminated while they are processing. What cost-effective solution can you use to reduce the number of incomplete process attempts?

A. Create a new Auto Scaling group with minimum and maximum of 2 and instances running web proxy software. Configure the VPC route table to route HTTP traffic to these web proxies.

B. Modify the application running on the instances to enable termination protection while it processes a task and disable it when the processing is complete.

C. Increase the minimum and maximum size for the Auto Scaling group, and change the scaling policies so they scale less dynamically.

D. Modify the application running on the instances to put itself into an Auto Scaling Standby state while it processes a task and return itself to InService when the processing is complete.

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

**Explanation/Reference:**

**QUESTION 289**
The operations team and the development team want a single place to view both operating system and application logs. How should you implement this using AWS services? (Choose two.)

A. Using AWS CloudFormation, create a CloudWatch Logs LogGroup and send the operating system and application logs of interest using the CloudWatch Logs Agent.

B. Using AWS CloudFormation and configuration management, set up remote logging to send events via UDP packets to CloudTrail.

C. Using configuration management, set up remote logging to send events to Amazon Kinesis and insert these into Amazon CloudSearch or Amazon Redshift, depending on available analytic tools.

D. Using AWS CloudFormation, create aCloudWatch Logs LogGroup. Because the Cloudwatch Log agent automatically sends all operating system logs, you only have to configure the application logs for sending off-machine.
E. Using AWS CloudFormation, merge the application logs with the operating system logs, and use IAM Roles to allow both teams to have access to view console output from Amazon EC2.

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

**Explanation/Reference:**

**QUESTION 290**
The project you are working on currently uses a single AWS CloudFormation template to deploy its AWS infrastructure, which supports a multi-tier web application. You have been tasked with organizing the AWS CloudFormation resources so that they can be maintained in the future, and so that different departments such as Networking and Security can review the architecture before it goes to Production. How should you do this in a way that accommodates each department, using their existing workflows?

A. Organize the AWS CloudFormation template so that related resources are next to each other in the template, such as VPC subnets and routing rules for Networking and security groups and IAM information for Security.
B. Separate the AWS CloudFormation template into a nested structure that has individual templates for the resources that are to be governed by different departments, and use the outputs from the networking and security stacks for theapplication template that you control
C. Organize the AWS CloudFormation template so that related resources are next to each other in the template for each department's use, leverage your existing continuous integration tool to constantly deploy changes from all parties tothe Production environment, and then run tests for validation.
D. Use a custom application and the AWS SDK to replicate the resources defined in the current AWS CloudFormation template, and use the existing code review system to allow other departments to approve changes before altering theapplication for future deployments.

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

**Explanation/Reference:**

**QUESTION 291**
You currently run your infrastructure on Amazon EC2 instances behind an Auto Scaling group. All logs for you application are currently written to ephemeral storage. Recently your company experienced a major bug in code that made it through testing and was ultimately deployed to your fleet. This bug triggered your Auto Scaling group to scale up and back down before you could successfully retrieve the logs off your server to better assist you in troubleshooting the bug. Which technique should you use to make sure you are able to review your logs after your instances have shut down?

A. Configure the ephemeral policies on your Auto Scaling group to back up on terminate.
B. Configure your Auto Scaling policies to create a snapshot of all ephemeral storage on terminate.
C. Install the CloudWatch Logs Agent on your AMI, and configure CloudWatch Logs Agent to stream your logs.
D. Install the CloudWatch monitoring agent on your AMI, and set up new SNS alert for CloudWatch metrics that triggers the CloudWatch monitoring agent to backup all logs on the ephemeral drive.
E. Install the CloudWatch monitoring agent on your AMI, Update your Auto Scaling policy to enable automated CloudWatch Log copy.

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

**Explanation/Reference:**

**QUESTION 292**
Management has reported an increase in the monthly bill from Amazon web services, and they are extremely concerned with this increased cost. Management has asked you to determine the exact cause of this increase. After reviewing the billing report, you notice an increase in the data transfer cost. How can you provide management with a better insight into data transfer use?

A. Update your Amazon CloudWatch metrics to use five-second granularity, which will give better detailed metrics that can be combined with your billing data to pinpoint anomalies.
B. Use Amazon CloudWatch Logs to run a map-reduce on your logs to determine high usage and data transfer.
C. Deliver custom metrics to Amazon CloudWatch per application that breaks down application data transfer into multiple, more specific data points.
D. Using Amazon CloudWatch metrics, pull your Elastic Load Balancing outbound data transfer metrics monthly, and include them with your billing report to show which application is causing higher bandwidth usage.

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

**Explanation/Reference:**
Section: (none)

**QUESTION 293**
During metric analysis, your team has determined that the company's website is experiencing response times during peak hours that are higher than anticipated. You currently rely on Auto Scaling to make sure that you are scaling your environment during peak windows. How can you improve your Auto Scaling policy to reduce this high response time? (Choose two.)

A. Push custom metrics to CloudWatch to monitor your CPU and network bandwidth from your servers, which will allow your Auto Scaling policy to have better

fine-grain insight.

B. Increase your Auto Scaling group's number of max servers.

C. Create a script that runs and monitors your servers; when it detects an anomaly in load, it posts to an Amazon SNS topic that triggers Elastic Load Balancing to add more servers to the load balancer.

D. Push custom metrics to CloudWatch for your application that include more detailed information about your web application, such as how many requests it is handling and how many are waiting to be processed.

E. Update the CloudWatch metric used for your Auto Scaling policy, and enable sub-minute granularity to allow auto scaling to trigger faster.

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

**Explanation/Reference:**

**QUESTION 294**
You are responsible for your company's large multi-tiered Windows-based web application running on Amazon EC2 instances situated behind a load balancer. While reviewing metrics, you have started noticing an upwards trend for slow customer page load time. Your manager has asked you to come up with a solution to ensure that customer load time is not affected by too many requests per second.
Which technique would you use to solve this issue?



A. Re-deploy your infrastructure using an AWS CloudFormation template. Configure Elastic Load Balancing health checks to initiate a new AWS CloudFormation stack when health checks return failed.

B. Re-deploy your infrastructure using an AWS CloudFormation template. Spin up a second AWS CloudFormation stack. Configure Elastic Load Balancing SpillOver functionality to spill over any slow connections to the second AWSCloudFormation stack.

C. Re-deploy your infrastructure using AWS CloudFormation, Elastic Beanstalk, and Auto Scaling. Set up your Auto Scaling group policies to scale based on the number of requests per second as well as the current customer load time.

D. Re-deploy your application using an Auto Scaling template. Configure the Auto Scaling template to spin up a new Elastic Beanstalk application when the customer load time surpasses your threshold.

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

**Explanation/Reference:**

**QUESTION 295**
Your company has multiple applications running on AWS. Your company wants to develop a tool that notifies on-call teams immediately via email when an

alarm is triggered in your environment. You have multiple on-call teams that work different shifts, and the tool should handle notifying the correct teams at the correct times. How should you implement this solution?

A. Create an Amazon SNS topic and an Amazon SQS queue. Configure the Amazon SQS queue as a subscriber to the Amazon SNS topic. Configure CloudWatch alarms to notify this topic when an alarm is triggered. Create an AmazonEC2 Auto Scaling group with both minimum and desired Instances configured to 0. Worker nodes in this group spawn when messages are added to the queue. Workers then use Amazon Simple Email Service to send messages to your on call teams.
B. Create an Amazon SNS topic and configure your on-call team email addresses as subscribers. Use the AWS SDK tools to integrate your application with Amazon SNS and send messages to this new topic. Notifications will be sent to on-call users when a CloudWatch alarm is triggered.
C. Create an Amazon SNS topic and configure your on-call team email addresses as subscribers. Create a secondary Amazon SNS topic for alarms and configure your CloudWatch alarms to notify this topic when triggered. Create an HTTPsubscriber to this topic that notifies your application via HTTP POST when an alarm is triggered. Use the AWS SDK tools to integrate your application with Amazon SNS and send messages to the first topic so that on-call engineers receive alerts.
D. Create an Amazon SNS topic for each on-call group, and configure each of these with the team member emails as subscribers. Create another Amazon SNS topic and configure your CloudWatch alarms to notify this topic whentriggered. Create an HTTP subscriber to this topic that notifies your application via HTTP POST when an alarm is triggered. Use the AWS SDK tools to integrate your application with Amazon SNS and send messages to the correct team topic when on shift.

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



**Explanation/Reference:**
Section: (none)

**QUESTION 296**
Your company releases new features with high frequency while demanding high application availability. As part of the application's A/B testing, logs from each updated Amazon EC2 instance of the application need to be analyzed in near real-time, to ensure that the application is working flawlessly after each deployment. If the logs show arty anomalous behavior, then the application version of the instance is changed to a more stable one. Which of the following methods should you use for shipping and analyzing the logs in a highly available manner?

A. Ship the logs to Amazon S3 for durability and use Amazon EMR to analyze the logs in a batch manner each hour.
B. Ship the logs to Amazon CloudWatch Logs and use Amazon EMR to analyze the logs in a batch manner each hour.
C. Ship the logs to an Amazon Kinesis stream and have the consumers analyze the logs in a live manner.
D. Ship the logs to a large Amazon EC2 instance and analyze the logs in a live manner.
E. Store the logs locally on each instance and then have an Amazon Kinesis stream pull the logs for live analysis.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 297**
You have a code repository that uses Amazon S3 as a data store. During a recent audit of your security controls, some concerns were raised about maintaining the integrity of the data in the Amazon S3 bucket. Another concern was raised around securely deploying code from Amazon S3 to applications running on Amazon EC2 in a virtual private cloud. What are some measures that you can implement to mitigate these concerns? (Choose two.)

A. Add an Amazon S3 bucket policy with a condition statement to allow access only from Amazon EC2 instances with RFC 1918 IP addresses and enable bucket versioning.
B. Add an Amazon S3 bucket policy with a condition statement that requires multi-factor authentication in order to delete objects and enable bucket versioning.
C. Use a configuration management service to deploy AWS Identity and Access Management user credentials to the Amazon EC2 instances. Use these credentials to securely access the Amazon S3 bucket when deploying code.
D. Create an Amazon Identity and Access Management role with authorization to access the Amazon 53 bucket, and launch all of your application's Amazon EC2 instances with this role.
E. Use AWS Data Pipeline to lifecycle the data in your Amazon S3 bucket to Amazon Glacier on a weekly basis.
F. Use AWS Data Pipeline with multi-factor authentication to securely deploy code from the Amazon .5.3 bucket to your Amazon EC2 instances.



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

**Explanation/Reference:**

**QUESTION 298**
You have an application consisting of a stateless web server tier running on Amazon EC2 instances behind load balancer, and are using Amazon RDS with read replicas. Which of the following methods should you use to implement a selfhealing and cost-effective architecture? (Choose two.)

A. Set up a third-party monitoring solution on a cluster of Amazon EC2 instances in order to emit custom CloudWatch metrics to trigger the termination of unhealthy Amazon EC2 instances.
B. Set up scripts on each Amazon EC2 instance to frequently send ICMP pings to the load balancer in order to determine which instance is unhealthy and replace it.
C. Set up an Auto Scaling group for the web server tier along with an Auto Scaling policy that uses the Amazon RDS DB CPU utilization CloudWatch metric to scale the instances.
D. Set up an Auto Scaling group for the web server tier along with an Auto Scaling policy that uses the Amazon EC2 CPU utilization CloudWatch metric to scale the instances.

E. Use a larger Amazon EC2 instance type for the web server tier and a larger DB instance type for the data storage layer to ensure that they don't become unhealthy.
F. Set up an Auto Scaling group for the database tier along with an Auto Scaling policy that uses the Amazon RDS read replica lag CloudWatch metric to scale out the Amazon RDS read replicas.
G. Use an Amazon RDS Multi-AZ deployment.

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

**Explanation/Reference:**

**QUESTION 299**
Your application is currently running on Amazon EC2 instances behind a load balancer. Your management has decided to use a Blue/Green deployment strategy. How should you implement this for each deployment?

A. Set up Amazon Route 53 health checks to fail over from any Amazon EC2 instance that is currently being deployed to.
B. Using AWS CloudFormation, create a test stack for validating the code, and then deploy the code to each production Amazon EC2 instance.
C. Create a new load balancer with new Amazon EC2 instances, carry out the deployment, and then switch DNS over to the new load balancer using Amazon Route 53 after testing.
D. Launch more Amazon EC2 instances to ensure high availability, de-register each Amazon EC2 instance from the load balancer, upgrade it, and test it, and then register it again with the load balancer.

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

**Explanation/Reference:**

**QUESTION 300**
Your company currently runs a large multi-tier web application. One component is an API service that all other components of your application rely on to perform read/write operations. This service must have high availability and zero downtime during deployments.
Which technique should you use to provide cost-effective, zero-downtime deployments for this component?

A. Use an AWS CloudFormation template to re-deploy your application behind a load balancer, and launch a new AWS CloudFormation stack during each deployment. Update your load balancer to send traffic to the new stack, and thendeploy your software. Leave your old stacks running, and tag their resources with the version for rollback.

B. Re-deploy your application on Elastic Beanstalk. During deployment, create a new version of your application, and create a new environment running that version in Elastic BeanStalk. Finally, take advantage of the Elastic BeanstalkSwap CNAME operation to switch to the new environment.
C. Re-deploy your application behind a load balancer that uses Auto Scaling groups. Create a new identical Auto Scaling group and associate it to your Amazon Route53 zone. Configure Amazon Route53 to auto- weight traffic over to thenew Auto Scaling group when all instances are marked as healthy.
D. Re-deploy your application behind a load balancer using an AWS OpsWorks stack and use AWS OpsWorks stack versioning, during deployment create a new version of your application, tell AWS OpsWorks to launch the new versionbehind your load balancer, and when the new version is launched, terminate the old AWS OpsWorks stack.

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

**Explanation/Reference:**

**QUESTION 301**
You want to build a new search tool feature for your monitoring system that will allow your information security team to quickly audit all API calls in your AWS accounts. What combination of AWS services can you use to develop and automate the backend processes supporting this tool? (Choose three.)

A. Create an Amazon CloudSearch domain for API call logs. Configure the search domain so that it can be used to index API call logs for the search tool.
B. Use AWS CloudTrail to store API call logs in an Amazon S3 bucket. Configure an Amazon Simple Notification Service topic called "log-notification" that notifies subscribers when new logs are available. Subscribe an Amazon SQS queueto the topic.
C. Use Amazon Cloudwatch to ship AWS CloudTrail logs to your monitoring system.
D. Create an AWS Elastic Beanstalk application in worker role mode that uses an Amazon Simple Email Service (SES) domain to facilitate batch processing new API call log files retrieved from an Amazon S3 bucket into a search index.
E. Use AWS CloudTrail to store API call logs in an Amazon S3 bucket. Configure Amazon Simple Email Service (SES) to notify subscribers when new logs are available. Subscribe an Amazon SQS queue to the email domain.
F. Create Amazon Cloudwatch custom metrics for the API call logs. Configure a Cloudwatch search domain so that it can be used to index API call logs for the search tool.
G. Create an AWS Elastic Beanstalk application in worker role mode that uses an Amazon SQS queue to facilitate batch processing new API call log files retrieved from an Amazon S3 bucket into a search index.

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

**Explanation/Reference:**

**QUESTION 302**
You are using AWS Elastic Beanstalk to deploy your application and must make data stored on an Amazon Elastic Block Store (EBS) volume snapshot available to the Amazon Elastic Compute Cloud (EC2) instances. How can you modify your Elastic Beanstalk environment so that the data is added to the Amazon EC2 instances every time you deploy your application?

A. Add commands to a configuration file in the .ebextensions folder of your deployable archive that mount an additional Amazon EBS volume on launch. Also add a "BlockDeviceMappings" option, and specify the snapshot to use for theblock device in the Auto Scaling launch configuration.
B. Add commands to a configuration file in the .ebextensions folder of your deployable archive that uses the create-volume Amazon EC2 API or CLI to create a new ephemeral volume based on the specified snapshot and then mounts thevolume on launch.
C. Add commands to the Amazon EC2 user data that will be executed by eb-init, which uses the create- volume Amazon EC2 API or CLI to create a new Amazon EBS volume based on the specified snapshot, and then mounts the volumeon launch.
D. Add commands to the Chef recipe associated with your environment, use the create-volume Amazon EC2 API or CLI to create a new Amazon EBS volume based on the specified snapshot, and then mount the volume on launch.

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

**Explanation/Reference:**



**QUESTION 303**
You would like to run automated, continuous application level integration tests on all members of an Auto Scaling group. Which two options should you use? (Choose two.)

A. Use the AWS SDK to run the DescribeInstances API call on the Auto Scaling group, and then iterate over the members and remotely connect to each Amazon EC2 instance and run the integration tests.
B. Use the AWS SDK to run the DescribeAutoScalingInstances API call on the Auto Scaling Group, iterate over the members using the Describe Instances API call, remotely connect to each Amazon EC2 instance, and then run theintegration tests.
C. Set up a custom CloudWatch metric with the output of your integration tests that are run by a scheduled process on each instance, and then set up a CloudWatch alert for any failures.
D. Using an Auto Cycle Group lifecycle policy, define a scheduled task to run integration tests when a new Amazon EC2 instance enters the InService state.
E. Set up a custom CloudWatch metric that uses the output of the DescribeAutoScalingInstances API call to determine the HealthCheck status of the Amazon EC2 instances.
F. Using the Auto Cycle Group lifecycle policy, define a scheduled task to run integration tests on individual instances using the Amazon EC2 user data to export test data to CloudWatch Logs.

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

**Explanation**

**Explanation/Reference:**

**QUESTION 304**
Your application Amazon Elastic Compute Cloud (EC2) instances bootstrap by using a master configuration file that is kept in a version-enabled Amazon Simple Storage Service (S3) bucket. Which one of the following methods should you use to securely install the current configuration version onto the instances in a cost-effective way?

A. Create an Amazon DynamoDB table to store the different versions of the configuration file. Associate AWS Identity and Access Management (IAM) EC2 roles to the Amazon EC2 instances, and reference the DynamoDB table to get thelatest file from Amazon Simple Storage Service (S3).
B. Associate an IAM S3 role to the bucket, list the object versions using the Amazon S3 API, and then get the latest object.
C. Associate an IAM EC2 role to the instances, list the object versions using the Amazon S3 API, and then get the latest object.
D. Associate an IAM EC2 role to the instances, and then simply get the object from Amazon S3, because the default is the current version.
E. Store the IAM credentials in the Amazon EC2 user data for each instance, and then simply get the object from S3, because the default is the current version.

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



**Explanation/Reference:**

**QUESTION 305**
Your company operates a website for promoters to sell tickets for entertainment events. You are using a load balancer in front of an Auto Scaling group of web servers. Promotion of popular events can cause surges of website visitors. During scaling-out at these times, newly launched instances are unable to complete configuration quickly enough, leading to user disappointment. What options should you choose to improve scaling yet minimize costs? (Choose two.)

A. Create an AMI with the application pre-configured. Create a new Auto Scaling launch configuration using this new AMI, and configure the Auto Scaling group to launch with this AMI.
B. Use Auto Scaling pre-warming to launch instances before they are required. Configure pre-warming to use the CPU trend CloudWatch metric for the group.
C. Publish a custom CloudWatch memo from your application on the number of tickets sold, and create an Auto Scaling policy based on this.
D. Use the history of past scaling events for similar event sales to predict future scaling requirements. Use the Auto Scaling scheduled scaling feature to vary the size of the fleet.
E. Configure an Amazon S3 bucket for website hosting. Upload into the bucket an HTML holding page with its x-amz-website-redirect-location' metadata property set to the load balancer endpoint. Configure Elastic Load Balancing to redirect to the holding page when the load on web servers is above a certain level.

**Correct Answer:** AD

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

**Explanation/Reference:**

**QUESTION 306**
You are responsible for a popular file sharing application that uses Elastic Load Balancing to distribute traffic to an Amazon EC2 application tier deployed in an Auto Scaling group that runs across multiple Availability Zones. You currently record the number of user file transfers to a log file on the application server, and then write data points from the logs to an Amazon RDS MySQL instance. You are not happy with how your application scales, and want to implement a new scaling policy based on the average number of user file transfers in a 10-minute period instead of average CPU utilization in the last five minutes. What steps should you take to ensure that your application tier scales based on this new policy? (Choose two.)

A. Create a new CloudWatch alarm based on the Elastic Load Balancing "RequestCount" metric that triggers an Auto Scaling action to scale the application tier.
B. Create a new CloudWatch alarm based on a custom metric streaming from the Amazon RDS MySQL instance that triggers an Auto Scaling action to scale the application tier.
C. Create a new CloudWatch alarm based on a custom metric published from file transfer logs streaming to CloudWatch that triggers an Auto Scaling action to scale the application tier.
D. Create a new Auto Scaling launch configuration that includes an Amazon EC2 user data script that installs a CloudWatch Logs Agent on newly launched instances in the application tier. The agent will be configured to stream the filetransfers log tile to CloudWatch.
E. Create a new Auto Scaling launch configuration for the application tier that scales based on an Auto Scaling policy that reads the file transfer log data from the Amazon RIDS MySQL instance.
F. Create a new Auto Scaling launch configuration that includes an Amazon EC2 user data script that installs an Amazon RDS Logs Agent on newly launched instances in the application tier. The agent will be configured to stream the filetransfer data points to the Auto Scaling group.

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

**Explanation/Reference:**

**QUESTION 307**
Your DevOps team is responsible for a multi-tier, Windows-based web application consisting of web servers, Amazon RDS database instances, and a load balancer behind Amazon Route53. You have been asked by your manager to build a cost-effective rolling deployment solution for this web application. What method should you use?

A. Re-deploy your application on an AWS OpsWorks stack. Use the AWS OpsWorks done stack feature to allow updates between duplicate stacks.
B. Re-deploy your application on Elastic Beanstalk and take advantage of Elastic BeanStalk rolling updates.

C. Re-deploy your application using an AWS CloudFormation template, launch a new AWS CloudFormation stack during each deployment, and then tear down the old stack.
D. Re-deploy your application using an AWS CloudFormation template. Use AWS CloudFormation rolling deployment policies, create a new policy for your AWS CloudFormation stack, and initiate an update stack operation to deploy newcode.

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

**Explanation/Reference:**

**QUESTION 308**
You recently encountered a major bug in your Windows-based web application during a deployment cycle. During this failed deployment, it took the team four hours to roll back to a previously working state, which left customers with a poor user experience. During the post-mortem, your team discussed the need to provide a quicker way to roll back failed deployments. You currently run your web application on Amazon EC2 using Windows 2012R2 and use Elastic Load Balancing for your load balancing needs. Which technique should you use to solve this problem?

A. Create deployable versioned bundles of your application. Store the bundles on Amazon S3. Re-deploy your web application on Elastic Beanstalk, and enable the Elastic Beanstalk autorollback feature tied to CloudWatch metrics thatdefine failure.
B. Re-deploy your web application using an AWS OpsWorks stack, and use the AWS OpsWorks auto-rollback feature to initiate a rollback during failures.
C. Create deployable versioned bundles of your application. Store the bundle on Amazon S3. Re-deploy your web application using an AWS OpsWorks stack, and use AWS OpsWorks application versioning to initiate a rollback duringfailures.
D. Re-deploy your web application using Elastic Beanstalk, and use the Elastic Beanstalk application versions when deploying. During failures, re-deploy the previous version to the Elastic Beanstalk environment.
E. Re-deploy your web application using Elastic Beanstalk, and use the Elastic Beanstalk API to trigger a FailedDeployment API call to initiate a rollback to the previous version.

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

**Explanation/Reference:**

**QUESTION 309**
You have a high-traffic application running behind a load balancer with clients that are very sensitive to latency. How should you determine which back-end Amazon Elastic Compute Cloud application instances are causing increased latency so that they can be replaced?

A. By using the Elastic Load Balancing Latency CloudWatch metric.
B. By using the HTTP X-Forwarded-For header for requests from the load balancer.
C. By running a distributed load test to the load balancer.
D. By using the load balancer access logs.

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

**Explanation/Reference:**

**QUESTION 310**
Your company operates an application consisting of an AWS CloudFormation stack that contains a load balancer, an Auto Scaling group of web servers, and an Amazon RDS instance. To save time and costs, you update the current test stack when testing minor changes, and create a new stack for major changes. As part of the testing procedure of your application, each version needs to be registered once and only once with a Configuration Management Database (CMDB). What cost-effective solution should you choose to perform this registration?

A. Use Auto Scaling Leader Node functionality to notify the registration application from the UserData script of a single Instance. Use the AWS CloudFormation cfn-hup helper application to receive template updates on the leader node,which then notifies the CMDB.
B. Define an AWS: :CloudFormation::CustomResource in the AWS CloudFormation template, with the application version as one of its properties. Modify the CMDB to subscribe to the resource's creation and update notifications.
C. Define an AWS::CloudFormation::HttpRequest in the AWS CloudFormation template, and configure it to notify the CMDB on stack creation and update.
D. Define an AWS::EC2::Instance resource in the AWS CloudFormation template that is configured to run a UserData script to notify the CMDB and then terminate itself on completion.

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

**Explanation/Reference:**

**QUESTION 311**
You manage a three-tier web application consisting of an autoscaled web proxy tier, an autoscaled application tier, and an Amazon RDS database tier. You use a load balancer to distribute requests from end users to the web proxy tier and another, internal load balancer to distribute requests between the web tier and the application tier. After deploying a small database schema update, you notice that all of your web and application instances have been terminated. What may have caused this?

A. Your load balancers use an HTTP health check, and the page relies on retrieving data from your database.
B. Your load balancer use TCP health checks to provide application-level health checks.
C. The cooldown period of the Auto Scaling group is too short, so the instances do not have enough time to recover from an issue.
D. Your Auto Scaling group health check type is set to "EC2" to check that the instances themselves are healthy.

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

**Explanation/Reference:**
Section: (none)

**QUESTION 312**
Your organization has decided to implement a third-party configuration management tool that uses a master server from which nodes pull configuration. You have built a custom base Amazon Machine Image that already has the third-party configuration management agent installed. You want to use the same base AMI in Development, Test and Production environments, each of which has its own master server. How should you configure your Amazon EC2 instances to register with the correct master server on launch?

A. Create a tag for all instances that specifies their environment. When launching instances, provide an Amazon EC2 UserData script that gets this tag by querying the MetaData Service and registers the agent with the master.
B. Use Amazon CloudFormation to describe your environment. Configure an input parameter for the master server hostname/address, and use this parameter within an Amazon EC2 UserData script that registers the agent with the master.
C. Create a script on your third-party configuration management master server that queries the Amazon EC2 API for new instances and registers them with it.
D. Use Amazon Simple Workflow Service to automate the process of registering new instances with your master server. Use an Environment tag in Amazon EC2 to register instances with the correct master server.

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

**Explanation/Reference:**

**QUESTION 313**
You have been asked to handle a large data migration from multiple Amazon RDS MySQL instances to a DynamoDB table. You have been given a short amount of time to complete the data migration. What will allow you to complete this complex data processing workflow?

A. Create an Amazon Kinesis data stream, pipe in all of the Amazon RDS data, and direct the data toward a DynamoDB table.
B. Write a script in your language of choice, install the script on an Amazon EC2 instance, and then use Auto Scaling groups to ensure that the latency of the

migration pipelines never exceeds four seconds in any 15-minute period.

C. Write a bash script to run on your Amazon RDS instance that will export data into DynamoDB.

D. Create a data pipeline to export Amazon RDS data and import the data into DynamoDB.

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

**Explanation/Reference:**

**QUESTION 314**
Your application requires a fault-tolerant, low-latency and repeatable method to load configurations files via Auto Scaling when Amazon Elastic Compute Cloud (EC2) instances launch. Which approach should you use to satisfy these requirements?

A. Securely copy the content from a running Amazon EC2 instance.

B. Use an Amazon EC2 UserData script to copy the configurations from an Amazon Storage Services (S3) bucket.

C. Use a script via cfn-init to pull content hosted in an Amazon ElastiCache cluster.

D. Use a script via cfn-init to pull content hosted on your on-premises server.

E. Use an Amazon EC2 UserData script to pull content hosted on your on-premises server.



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

**Explanation/Reference:**

**QUESTION 315**
Currently, your deployment process consists of setting your load balancer to point to a maintenance page, turning off ea web application servers, deploying your code, turning the web application servers back on, and removing the maintenance page. Working with your development team, you've agreed that performing rolling deployments of your software would provide a better user experience and a more agile deployment process.
Which techniques could you use to provide a cost-effective rolling deployment process? (Choose two.)

A. Use the Amazon Elastic Cloud Compute (EC2) API to write a service to return a list of servers based on the tags for the application that needs deployment, and use Amazon Simple Queue Service to queue up all servers for a rollingdeployment.

B. Re-deploy your application on AWS Elastic Beanstalk, and use Elastic Beanstalk rolling deployments.

C. Re-deploy your application on an AWS OpsWorks stack, and take advantage of OpsWorks rolling deployments.

D. Re-deploy your application using an AWS CloudFormation template, launch a new CloudFormation stack during each deployment, and then tear down the old stack.
E. Re-deploy your application using an AWS CloudFormation template with Auto Scaling group, and use update policies to provide rolling updates.
F. Using Amazon Simple Workflow Service, create a workflow application that talks to the Amazon EC2 API to deploy your new code in a rolling fashion.

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

**Explanation/Reference:**

**QUESTION 316**
You manage a web advertising platform on a single AWS account. This platform produces realtime ad-click data that you store as objects in an Amazon S3 bucket called "dick-data." Your advertising partners want to use Amazon Elastic MapReduce in their own AWS accounts to do analytics on the ad-click data. They have asked for immediate access to the ad-dick data so that they can run analytics.
Which two choices are required to facilitate secure access to this data? (Choose two.)

A. Create a cross-account TAM role with a trust policy that contains partner AWS account IDs and a unique external ID.
B. Create a new IAM group for AWS Data Pipeline users with a trust policy that contains partner AWS account IDs.
C. Configure an Amazon S3 bucket policy for the "click-data" bucket that allows Read-Only access to the objects, and associate this policy with an IAM role.
D. Configure the Amazon S3 bucket access control list to allow access to the partners Amazon Elastic MapReduce cluster.
E. Configure AWS Data Pipeline in the partner AWS accounts to use the web Identity Federation API to access data in the "click-data" bucket.
F. Configure AWS Data Pipeline to transfer the data from the "click-data" bucket to the partner's Amazon Elastic MapReduce cluster.

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

**Explanation/Reference:**

**QUESTION 317**
You run a SIP-based telephony application that uses Amazon EC2 for its web tier and uses MySQL on Amazon RDS as its database. The application stores only the authentication profile data for its existing users in the database and therefore is read-intensive. Your monitoring system shows that your web instances and the database have high CPU utilization. Which of the following steps should you take in order to ensure the continual availability of your application? (Choose two.)

A. Use a CloudFront RTMP download distribution with the application tier as the origin for the distribution.

B. Set up an Auto Scaling group for the application tier and a policy that scales based on the Amazon EC2 CloudWatch CPU utilization metric.
C. Vertically scale up the Amazon EC2 instances manually.
D. Set up an Auto Scaling group for the application tier and a policy that scales based on the Amazon RDS CloudWatch CPU utilization metric.
E. Switch to General Purpose (SSD) Storage from Provisioned IOPS Storage (PIOPS) for the Amazon RDS database.
F. Use multiple Amazon RDS read replicas.

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

**Explanation/Reference:**

**QUESTION 318**
Your team is responsible for an AWS Elastic Beanstalk application. The business requires that you move to a continuous deployment model, thus releasing updates to the application multiple times per day with zero downtime.
What should you do to enable this and still be able to roll back to the previous version almost immediately in an emergency?

A. Enable roiling updates in the Elastic Beanstalk environment and set an appropriate pause time for application startup.
B. Create a second Elastic Beanstalk environment that runs the new application version, and swap the environment CNAMEs.
C. Configure the application to poll for a new application version in your code repository; download and install the new version to each running Elastic Beanstalk instance.
D. Create a second Elastic Beanstalk environment with the new application version, and configure the old environment to use the HTTP 301 response code to redirect clients to the new environment.

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

**Explanation/Reference:**

**QUESTION 319**
Your Company wants to perform A/B testing on a new website feature for 20 percent of its users. The website uses CloudFront for whole site delivery, with some content cached for up to 24 hours. How do you enable this testing for the required proportion of users while minimizing performance impact?

A. Configure the web servers to handle two domain names. The feature is switched on or off depending on which domain name is used for a request. Configure a CloudFront origin for each domain name, and configure the CloudFrontdistribution to use one origin for 20 percent of users and the other origin for the other 80 percent.

B. Configure the CloudFront distribution to forward a cookie specific to this feature. For requests where the cookie is not set, the web servers set its value to "on" for 20 percent of responses and "off" for 80 percent. For requests where thecookie is set, the web servers use Its value to determine whether the feature should be on or off for the response.

C. Create a second stack of web servers that host the website with the feature on. Using Amazon Route53, create two resource record sets with the same name: one with a weighting of "1" and a value of this new stack; the other a weightingof "4" and a value of the existing stack. Use the resource record set's name as the CloudFront distribution's origin.

D. Invalidate all of the CloudFront distribution's cache items that the feature affects. On future requests, the web servers create responses with the feature on for 20 percent of users, and off for 80 percent. The web servers set "Cache-Control: no-cache" on all of these responses.

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

**Explanation/Reference:**

**QUESTION 320**
You have been asked to use your departments existing continuous Integration (CI) tool to test a three-tier web architecture defined In an AWS CloudFormation template. The tool already supports AWS APIs and can launch new AWS CloudFormation stacks after polling version control. The CI tool reports on the success of the AWS CloudFormation stack creation by using the Describe Stacks API to look for the CREATE COMPLETE status. The architecture tiers defined in the template consist of:
- One load balancer
- Five Amazon EC2 instances running the web application
- One multi-AZ Amazon ROS instance
How would you implement this? (Choose two.)



A. Define a WaitCondition and a WaitConditionHandle for the output of a UserData command that does sanity checking of the application's post-install state.

B. Define a CustomResource and write a script that runs architecture-level Integration tests through the load balancer to the application and database for the state of multiple tiers.

C. Define a WaitCondition and use a WaitConditionHandle that leverages the AWS SDK to run the DescribeStacks API call until the CREATE COMPLETE status is returned.

D. Define a CustomResource that leverages the AWS SDK to run the DescribeStacks API call until the 'CREATE COMPLETE status is returned.

E. Define a UserDataHandle for the output of a UserData command that does sanity checking of the application's post-install state and runs integration tests on the state of multiple tiers through the load balancer to the application.

F. Define a UserDataHandle for the output of a CustomResource that does sanity checking of the application's post-install state.

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

**Explanation/Reference:**

**QUESTION 321**
You are building a large, multi-tenant SaaS (software-as-a-service) application with a component that fetches data to process from a customer-specific Amazon S3 bucket in their account. How should you ensure that your application follows security best practices and limits risk when fetching data from customer-owned Amazon S3 buckets?

A. Have users create an IAM user with a policy that grants read-only access to the Amazon S3 bucket required by your application, and store the corresponding access keys in an encrypted database that holds their account data.
B. Have users create a cross-account IAM role with a policy that grants read-only access to the Amazon S3 bucket required by your application to the AWS account ID running your production Sass application.
C. Have users create an Amazon S3 bucket policy that grants read-only access to the Amazon S3 bucket required by your application, and securely store the corresponding access keys in the database holding their account data.
D. Have users create an Amazon S3 bucket policy that grants read-only access to the Amazon S3 bucket required by your application and limits access to the public IP address of the SaaS application.

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



**Explanation/Reference:**

**QUESTION 322**
You have a fleet of Elastic Compute Cloud (EC2) instances in an Auto Scaling group. All of these instances are running Microsoft Windows Server 2012 backed by Amazon Elastic Block Store (EBS). These instances were launched through AWS CloudFormation. You have determined that your instances are underutilized, and in order to save some money, have decided to modify the instance type of the fleet. In which of the following ways can you achieve the desired result during a scheduled maintenance window? (Choose two.)

A. Create a new Auto Scaling launch configuration specifying the new instance type, associate it to the existing Auto Scaling group, and terminate the running instances.
B. Identify the new instance type in the user data and restart the running instances one at a time.
C. Use the AWS Command Line Interface (CLI) to modify the instance type of each running instance.
D. Change the instance type in the AWS CloudFormation template that was used to create the Amazon EC2 instances, and then update the stack.
E. Take snapshots of the running instances, and launch new instances based on those snapshots.

**Correct Answer:** AD

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

**Explanation/Reference:**

**QUESTION 323**
You run a large number of applications on Amazon EC2 instances. Each application has associated metadata, such as cost center, support contact, and application ID. Many applications usually co-exist on each Amazon EC2 instance, so the amount of metadata per instance can range from 10 to 200 items. The customer wants to be able to quickly access this metadata using an API without logging into the instances. Which of the following options will satisfy their requirements? (Choose two.)

A. Create individual Amazon EC2 tags for each metadata item, and associate them with the Amazon EC2 instances. Access the metadata by using the ec2-describe-instance API call.
B. Create compound Amazon EC2 tags for the metadata items, where multiple items are joined together in individual tags, and associate them with the Amazon EC2 instances. Access the metadata by using the ec2-describe-tags API call.
C. Create a DynamoDB table to hold the metadata, and associate it with the Amazon EC2 instance IDs running the applications. Access the metadata by querying the database via the DynamoDB API.
D. As part of the Amazon EC2 Instance bootstrapping process, add the metadata to the Amazon EC2 user data. Access the metadata by using the ec2-describe-instance API call.
E. As part of the Amazon EC2 instance bootstrapping process, add the metadata to the Amazon EC2 user data. Access the metadata by accessing its loopback address from a management instance in the same VPC.



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

**Explanation/Reference:**

**QUESTION 324**
You have an application running on multiple Amazon EC2 instances within an Auto Scaling group. You notice that instances are being re-spawned as their health checks are failing in Amazon EC2. However, before you have a chance to diagnose the issue, the affected instances are being terminated by the Auto Scaling service. You receive notifications of health checks failing and investigate within 20 minutes. However, this is not enough time to troubleshoot the issue.
What should you change that will enable you to troubleshoot the instance before it is terminated by the Auto Scaling service, while keeping costs minimal?

A. Install the Amazon CloudWatch Logs Agent on the instance and configure application and system logs to be sent to the CloudWatch Logs service.
B. Configure an Amazon SNS topic and associate it with your Auto Scaling group's CloudWatch alarms. Configure an Amazon SQS queue as a subscriber of this topic, and then create a fleet of Amazon EC2 workers that poll this queue andinstruct the Amazon EC2 Auto Scaling API to remove the instance from the Auto Scaling group when an alarm is triggered.

C. Create an Auto Scaling Group lifecycle hook to hold the instance in a terminating:wait state until you have completed any troubleshooting. When you have completed troubleshooting, wait for the terminating state to expire, or notify toScaling to complete the lifecycle hook and terminate the Instance.
D. Change the "DeleteOnTermination" flag to false in the Auto Scaling group configuration to ensure that instances are not deleted in the future.

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

**Explanation/Reference:**

**QUESTION 325**
You set up a scalable continuous integration platform on AWS. The platform consists of a master node that can delegate project build jobs to multiple slave nodes, all running on Amazon EC2. The build output will be stored in Amazon S3. You always have five slave nodes deployed. Each slave node can handle 10 build jobs simultaneously. Your master node publishes a custom Amazon CloudWatch metric with the name "RunningBuildiobs" that Slows you to programmatically track how many build jobs are running across your platform.
Which two configuration options will allow you to flexibly scale your platform to support more than 50 simultaneous build jobs while minimizing costs? (Choose two.)

A. Place your fleet of slave nodes in an Auto Scaling group. Configure a CloudWatch alarm that triggers an Auto Scaling policy to launch Amazon EC2 Instances when "RunningBuildJobs" is greater than 45 for more than five minutes.
B. Configure a CloudWatch alarm that sends an alert when "RunningBuildJobs" is greater than 45 for more than five minutes. Use Amazon Simple Queue Service to process additional build jobs when the CloudWatch alarm is triggered.
C. Configure your fleet of slave nodes to fully utilize all of your purchased Amazon EC2 Heavy Utilization Reserved Instances. Configure a CloudWatch alarm that launches new Amazon EC2 instances when "RunningBuildJobs" is less than40 for more than five minutes.
D. Run your fleet of slave nodes in an Auto Scaling group. Configure a Cloudwatch alarm that launches new Amazon EC2 Dedicated Instances when "RunningBuildJobs" is less than 40 for more than five minutes.
E. Place your fleet of slave nodes in an Auto Scaling group. Configure a CloudWatch alarm that triggers an Auto Scaling policy to terminate Amazon EC2 instances when "RunningBuildJobs" is less than 40 for more than five minutes.

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

**Explanation/Reference:**

**QUESTION 326**
You have just come from your Chief Information Security Officer's (CISO) office with the instructions to provide an audit report of all AWS network rules used by the organization's Amazon EC2 instances. You have discovered that a single Describe-Security-Groups API call will return all of an account's security groups and

rules within a region. You create the following pseudo-code to create the required report:
- Parse "aws ec2 describe-security-groups" output
- For each security group
- Create report of ingress and egress rules
Which two additional pieces of logic should you include to meet the CISO's requirements? (Choose two.)

A. Parse security groups in each region.
B. Parse security groups in each Availability Zone and region.
C. Evaluate VPC network access control lists.
D. Evaluate AWS CloudTrail logs.
E. Evaluate Elastic Load Balancing access control lists.
F. Parse CloudFront access control lists.

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

**Explanation/Reference:**



**QUESTION 327**
You are responsible for a large-scale video transcoding system that operates with an Auto Scaling group of video transcoding workers. The Auto Scaling group is configured with a minimum of 750 Amazon EC2 instances and a maximum of
1000 Amazon EC2 instances. You are using Amazon SQS to pass a message containing the URI for a video stored in Amazon S3 to the transcoding workers. An Amazon CloudWatch alarm has notified you that the queue depth is becoming very large. How can you resolve the alarm without the risk of increasing the time to transcode videos? (Choose two.)

A. Create a second queue in Amazon SQS.
B. Adjust the Amazon CloudWatch alarms for a higher queue depth.
C. Create a new Auto Scaling group with a launch configuration that has a larger Amazon EC2 instance type.
D. Add an additional Availability Zone to the Auto Scaling group configuration.
E. Change the Amazon CloudWatch alarm so that it monitors the CPU utilization of the Amazon EC2 instances rather than the Amazon SQS queue depth.
F. Adjust the Auto Scaling group configuration to increase the maximum number of Amazon EC2 instances.

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

**Explanation/Reference:**

**QUESTION 328**
You have been tasked with deploying a solution for your company that will store images, which the marketing department will use for its campaigns. Employees are able to upload images via a web interface, and once uploaded, each image must be resized and watermarked with the company logo. Image resize and watermark is not time-sensitive and can be completed days after upload if required. How should you design this solution in the most highly available and costeffective way?

A. Configure your web application to upload images to the Amazon Elastic Transcoder service. Use the Amazon Elastic Transcoder watermark feature to add the company logo as a watermark on your images and then to upload the finalimages into an Amazon S3 bucket.
B. Configure your web application to upload images to Amazon S3, and send the Amazon S3 bucket URI to an Amazon SQS queue. Create an Auto Scaling group and configure it to use Spot instances, specifying a price you are willing topay. Configure the instances in this Auto Scaling group to poll the SQS queue for new images and then resize and watermark the image before uploading the final images into Amazon S3.
C. Configure your web application to upload images to Amazon S3, and send the S3 object URI to an Amazon SQS queue. Create an Auto Scaling launch configuration that uses Spot instances, specifying a price you are willing to pay.Configure the instances in this Auto Scaling group to poll the Amazon SQS queue for new images and then resize and watermark the image before uploading the new images into Amazon S3 and deleting the message from the Amazon SQS queue.
D. Configure your web application to upload images to the local storage of the web server. Create a cronjob to execute a script daily that scans this directory for new files and then uses the Amazon EC2 Service API to launch 10 newAmazon EC2 instances, which will resize and watermark the images daily.



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

**Explanation/Reference:**

**QUESTION 329**
You run a small online consignment marketplace. Interested sellers complete an online application in order to allow them to sell their products on your website. Once approved, they can post their product using a custom interface. From that pant, you manage the shopping cart process so that when a buyer decides to buy a product, you handle the billing and coordinate the shipping. Part of this process requires sending emails to the buyer and the seller at different stages. Your system has been running on AWS for a few months. Occasionally, products are shipped before payment cleared and emails are sent out of order. Furthermore, sometimes credit cards are being charged twice. How can you resolve these problems?

A. Use the Amazon Simple Queue Service (SQS), and use a different set of workers for each task.
B. Use the Amazon Simple Workflow Service (SWF), and use a different set of workers for each task.
C. Use the Simple Email Service (SES) to control the correct order of email delivery.
D. Use the AWS Data Pipeline service to control the process flow of the various tasks.

E. Use the Amazon Simple Queue Service (SQS), and use a single set of workers for each task.

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

**Explanation/Reference:**

**QUESTION 330**
Your application has an Auto Scaling group of m3.large instances running an application that receives messages born an Amazon SQS queue. After a while, the number of instances reaches the maximum set for the group and the number of messages on the queue continues to increase. You have discovered that a third-party library used by the application has a bug that causes a memory leak. What cost-effective steps can you take to continue message processing while the library developer fixes the bug?

A. Enable Elastic Load Balancing health checks for the Auto Scaling group. When Elastic Load Balancing has detected a failure, Auto Scaling will terminate the failing application's instance and launch a new one.
B. Use Amazon EC2 instance memory usage CloudWatch metrics to raise alerts when they reach a defined level and send a message to Auto Scaling to fail the instance health check.
C. Use application monitoring on the instance to restart the application when memory usage reaches a defined level.
D. Create a new Auto Scaling launch configuration to use the r3.large instance type. Update the Auto Scaling group with the new launch configuration.

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

**Explanation/Reference:**

**QUESTION 331**
You are in charge of a large-scale highly available multi-tier web application infrastructure. This architecture consists of Amazon Route53 with a load balancer and multiple Amazon EC2 instances. You have been tasked to come up with a process to provide Blue/Green style deployments.
Which technique should you use to deliver this new requirement?

A. Using Elastic Beanstalk re-deploy your application and configure Elastic Beanstalk Deployment types, and then use Amazon Route53's alias resource record set to swap between Elastic Beanstalk deployment types.
B. Re-deploy your application behind a load balancer using an AWS CloudFormation template, launch a new AWS CloudFormation stack during each deployment, update your Amazon Route53 alias resource record set to point to the newload balancer, and finally, terminate your old AWS CloudFormation stack.

C. Re-deploy your application behind a load balancer using Auto Scaling groups, create a new identical Auto Scaling group, and associate it to the load balancer. During deployment, create a new Amazon Route53 hosted zone, add this newload balancer to the zone in an alias resource record set, and then remove your old Auto Scaling group.

D. Re-deploy your application behind a load balancer using an OpsWorks stack, and use AWS OpsWorks stack versioning. During deployment, create a new version of your application, tell OpsWorks to launch the new version behind yourload balancer, and when the new version launches, update your Amazon Route53 alias resource retort to point to the new load balancer.

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

**Explanation/Reference:**

**QUESTION 332**
Your application uses Amazon SQS and Auto Scaling to process background jobs. The Auto Scaling policy is based on the number of messages in the queue, with a maximum Instance count of 100. Since the application was launched, the group has never scaled above 50. The Auto Scaling group has now scaled to 100, the queue size is increasing, and very few Jobs are being completed. The number of messages being sent to the queue is at normal levels. What should you do to identify why the queue size is unusually high, and to reduce it?

A. Temporarily increase the Auto Scaling group's desired value to 200. When the queue size has been reduced, reduce it to 50.

B. Analyze the application logs to identify possible reasons for message processing failure and resolve the cause for failures.

C. Create additional Auto Scaling groups, enabling the processing of the queue to be performed in parallel.

D. Analyze CloudTrail logs for Amazon SQS to ensure that the instances' Amazon EC2 role has permission to receive messages from the queue.

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

**Explanation/Reference:**

**QUESTION 333**
You have a web application that is currently running on a collection of micro instance types in a single AZ behind a single load balancer. You have an Auto Scaling group configured to scale from 2 to 64 instances. When reviewing your
CloudWatch metrics, you see that sometimes your Auto Scaling group is running 64 micro instances. The web application is reading and writing to a DynamoDB-configured backend and configured with 800 Write Capacity Units and 800
Read Capacity Units. Your customers are complaining that they are experiencing long load times when viewing your website. You have investigated the DynamoDB CloudWatch metrics; you are under the provisioned Read and write Capacity Units and there is no throttling.
How do you scale your service to improve the load times and ensure the principles of high availability?

A. Change your Auto Scaling group configuration to include multiple AZs.
B. Change your Auto Scaling group configuration to include multiple AZs, and increase the number of Read Capacity Units in your DynamoDB table by a factor of three, because you will need to be calling DynarnoDB from three AZs.
C. Add a second load balancer to your Auto Scaling group so that you can support more inbound connections per second.
D. Change your Auto Scaling group configuration to use larger instances and include multiple AZ's instead of one.

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

**Explanation/Reference:**

**QUESTION 334**
Your social media marketing application has a component written in Ruby running on AWS Elastic Beanstalk. This application component posts messages to social media sites in support of various marketing campaigns. Your management now requires you to record replies to these social media messages to analyze the effectiveness of the marketing campaign in comparison to past and future efforts. You have already developed a new application component to interface with the social media site APIs in order to read the replies.
Which process should you use to record the social media replies in a durable data store that can be accessed at any time for analysis of historical data?

A. Deploy the new application component in an Auto Scaling group of Amazon Elastic Compute Cloud (EC2) Instances, read the data from the social media sites, store it with Amazon Elastic Block Store, and use AWS Data Pipeline topublish it to Amazon Kinesis for analytics.
B. Deploy the new application component as an Elastic Beanstalk application, read the data from the social media sites, store it in Amazon DynamoDB, and use Apache Hive with Amazon Elastic MapReduce for analytics.
C. Deploy the new application component in an Auto Scaling group of Amazon EC2 instances, read the data from the social media sites, store it in Amazon Glacier, and use AWS Data Pipeline to publish it to Amazon Redshift for analytics.
D. Deploy the new application component as an Amazon Elastic Beanstalk application, read the data from the social media site, store it with Amazon Elastic Block Store, and use Amazon Kinesis to stream the data to Amazon CloudWatch for analytics.

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

**Explanation/Reference:**

**QUESTION 335**
A web application is being actively developed by multiple development teams within your organization. You have created a self-service portal-driven by AWS

CloudFormation and the AWS APIs-that allows testers to select a code branch containing a new feature that they want to test. The portal will then provision an environment and deploy the right branch of code to it. Recently you have noticed that a large number of environments contain broken builds. You want to introduce a set of automated browser tests that are executed on a new environment before the environment is available to the tester. This way a tester does not waste time trying to test new features in a broken environment. Select a suitable way to implement such a feature into the existing self-service portal:

A. Specify your automated tests in the "tests" section of the AWS CloudFormation template. AWS CloudFormation will then execute the tests on your behalf as part of the environment build.
B. Configure a centralized test server that hosts an automated browser testing framework. Use an AWS CloudFormation custom resource to notify the centralized test server, via an Amazon SNS topic, that a new environment has beeninitialized. The centralized test server can then execute the tests before sending the results back to the AWS CloudFormation service.
C. Pass the test scripts to the cfn-init service via the "tests" section of the AWS::CloudFormation::Init metadata. Cfn-init will then execute these tests and return the result to the AWS CloudFormation service.
D. Configure a centralized test server that hosts an automated browser testing framework. Include an Amazon SES email resource under the outputs section of your AWS CloudFormation template. This we send an email to your centralizedtest server, informing it that the environment is ready for tests.

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

**Explanation/Reference:**



**QUESTION 336**
You have written a server-side Node.Js application and a web application with an HTML/JavaScript front end that uses the Angular.js framework. The server-side application connects to an Amazon Redshift cluster, issues queries, and then returns the results to the front end for display. Your user base is very large and distributed, but it is important to keep the cost of running this application low. Which deployment strategy is both technically valid and the most cost-effective?

A. Deploy an AWS Elastic Beanstalk application with two environments: one for the Node.js application and another for the web front end. Launch an Amazon Redshift cluster, and point your application to its Java Database Connectivity(JDBC) endpoint.
B. Deploy an AWS OpsWorks stack with three layers: a static web server layer for your front end, a Node.js app server layer for your server-side application, and a Redshift DB layer for your Amazon Redshift duster.
C. Upload the HTML, CSS, images, and JavaScript for the front end to an Amazon Simple Storage Service (S3) bucket. Create an Amazon CloudFront distribution with this bucket as its origin. Use AWS Elastic Beanstalk to deploy theNode.js application. Launch an Amazon Redshift cluster, and point your application to its JDBC endpoint.
D. Upload the HTML, CSS, images, and JavaScript for the front end, plus the Node.js code for the server-side application, to an Amazon S3 bucket. Create a CloudFront distribution with this bucket as its origin. Launch an Amazon Redshiftcluster, and point your application to its JDBC endpoint.
E. Upload the HTML, CSS, images, and JavaScript for the front end to an Amazon S3 bucket. Use AWS Elastic Beanstalk to deploy the Node.js application. Launch an Amazon Redshift cluster, and point your application to its JDBCendpoint.

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

**Explanation/Reference:**

**QUESTION 337**
You are building an AWS CloudFormation template for a multi-tier web application. The user data of your Linux web server resource contains a complex script that can take a long time to run. Which techniques could you use to ensure that these servers are fully configured and running before attaching them to the load balancer? (Choose two.)

A. Launch your Linux servers from a nested stack that is called from within the load balancer resource in your AWS CloudFormation template.
B. Add an AWS CloudFormation Wait Condition that depends on the web server resource. When the UserData script finishes on the web servers, use curl to send a signal the Wait Condition at http://169.254.169.254/waithandle/.
C. Add an AWS CloudFormation wait Condition that depends on the web server resource. When the UserData script finishes on the web servers, use curl to signal to the Wait Condition pre-signed URL that they are ready.
D. In your AWS CloudFormation template, position the load balancer resource JSON block directly below your Linux server resource.
E. Add an AWS CloudFormation Wait Condition that depends on the web server resource. When the UserData script finishes on the web servers, use the command "cfn-signal" to signal that they are ready.



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

**Explanation/Reference:**

**QUESTION 338**
Customers have recently been complaining that your web application has randomly stopped responding. During a deep dive of your logs, the team has discovered a major bug in your new Java web application. This bug is causing a memory leak that eventually causes the application to crash. Your web application runs on Amazon EC2 and was built with AWS CloudFormation. Which techniques should you use to help detect these problems faster, as well as help eliminate the server's unresponsiveness? (Choose two.)

A. Update your AWS CloudFormation configuration and enable a CustomResource that uses cfnsignal to detect memory leaks.
B. Update your CloudWatch metric granularity config for all Amazon EC2 memory metrics to support five- second granularity. Create a CloudWatch alarm that triggers an Amazon SNS notification to page your team when the applicationmemory becomes too large.
C. Update your AWS CloudFormation configuration to take advantage of Auto Scaling groups. Configure an Auto Scaling group policy to trigger off your custom CloudWatch metrics.

D. Create a custom CloudWatch metric that you push your JVM memory usage to. Create a Cloudwatch alarm that triggers an Amazon SNS notification to page your team when the application memory usage becomes too large.
E. Update your AWS CloudFormation configuration to take advantage of CloudWatch metrics Agent. Configure the CloudWatch Metrics Agent to monitor memory usage and trigger an Amazon SNS alarm.

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

**Explanation/Reference:**

**QUESTION 339**
You have an ASP.NET web application running in Amazon Elastic Beanstalk. Your next version of the application requires a third-party Windows Installer package to be installed on the instance on first boot and before the application launches.
Which options are possible? (Choose two.)

A. In the application's Global.asax file, run msiexec.exe to install the package using Process.Start() in the Application Start event handler.
B. In the source bundle's .ebextensions folder, create a file with a .config extension. In the file, under the "packages" section and "msi" package manager, include the package's URL.
C. Launch a new Amazon EC2 instance from the AMI used by the environment. Log into the instance, install the package and run sysprep. Create a new AMI. Configure the environment to use the new AMI.
D. In the environment's configuration, edit the instances configuration and add the package's URL to the "Packages" section.
E. In the source bundle's .ebextensions folder, create a "Packages" folder. Place the package in the folder.

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

**Explanation/Reference:**
Section: (none)

**QUESTION 340**
For AWS Auto Scaling, what is the first transition state an instance enters after leaving steady state when scaling in due to health check failure or decreased load?

A. Terminating
B. Detaching
C. Terminating:Wait

D. EnteringStandby

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

**Explanation/Reference:**
When Auto Scaling responds to a scale in event, it terminates one or more instances. These instances are detached from the Auto Scaling group and enter the Terminating state.
Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingGroupLifecycle.html

**QUESTION 341**
You are hired as the new head of operations for a SaaS company. Your CTO has asked you to make debugging any part of your entire operation simpler and as fast as possible. She complains that she has no idea what is going on in the complex, service-oriented architecture, because the developers just log to disk, and it's very hard to find errors in logs on so many services. How can you best meet this requirement and satisfy your CTO?

A. Copy all log files into AWS S3 using a cron job on each instance. Use an S3 Notification Configuration on the <code>PutBucket</code> event and publish events to AWS Lambda. Use the Lambda to analyze logs as soon as they comein and flag issues.
B. Begin using CloudWatch Logs on every service. Stream all Log Groups into S3 objects. Use AWS EMR cluster jobs to perform ad-hoc MapReduce analysis and write new queries when needed.
C. Copy all log files into AWS S3 using a cron job on each instance. Use an S3 Notification Configuration on the <code>PutBucket</code> event and publish events to AWS Kinesis. Use Apache Spark on AWS EMR to perform at-scalestream processing queries on the log chunks and flag issues.
D. Begin using CloudWatch Logs on every service. Stream all Log Groups into an AWS Elasticsearch Service Domain running Kibana 4 and perform log analysis on a search cluster.

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

**Explanation/Reference:**
The Elasticsearch and Kibana 4 combination is called the ELK Stack, and is designed specifically for real-time, ad-hoc log analysis and aggregation. All other answers introduce extra delay or require pre-defined queries. Amazon
Elasticsearch Service is a managed service that makes it easy to deploy, operate, and scale Elasticsearch in the AWS Cloud. Elasticsearch is a popular open-source search and analytics engine for use cases such as log analytics, real-time application monitoring, and click stream analytics.
Reference: https://aws.amazon.com/elasticsearch-service/

**QUESTION 342**
When thinking of AWS Elastic Beanstalk's model, which is true?

A. Applications have many deployments, deployments have many environments.

B. Environments have many applications, applications have many deployments.
C. Applications have many environments, environments have many deployments.
D. Deployments have many environments, environments have many applications.

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

**Explanation/Reference:**
Applications group logical services. Environments belong to Applications, and typically represent different deployment levels (dev, stage, prod, fo forth). Deployments belong to environments, and are pushes of bundles of code for the environments to run.
Reference: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

**QUESTION 343**
You work for a company that automatically tags photographs using artificial neural networks (ANNs), which run on GPUs using C++. You receive millions of images at a time, but only 3 times per day on average. These images are loaded into an AWS S3 bucket you control for you in a batch, and then the customer publishes a JSON-formatted manifest into another S3 bucket you control as well. Each image takes 10 milliseconds to process using a full GPU. Your neural network software requires 5 minutes to bootstrap. Image tags are JSON objects, and you must publish them to an S3 bucket. Which of these is the best system architectures for this system?

A. Create an OpsWorks Stack with two Layers. The first contains lifecycle scripts for launching and bootstrapping an HTTP API on G2 instances for ANN image processing, and the second has an always-on instance which monitors the S3manifest bucket for new files. When a new file is detected, request instances to boot on the ANN layer. When the instances are booted and the HTTP APIs are up, submit processing requests to individual instances.
B. Make an S3 notification configuration which publishes to AWS Lambda on the manifest bucket. Make the Lambda create a CloudFormation Stack which contains the logic to construct an autoscaling worker tier of EC2 G2 instances withthe ANN code on each instance. Create an SQS queue of the images in the manifest. Tear the stack down when the queue is empty.
C. Deploy your ANN code to AWS Lambda as a bundled binary for the C++ extension. Make an S3 notification configuration on the manifest, which publishes to another AWS Lambda running controller code. This controller code publishesall the images in the manifest to AWS Kinesis. Your ANN code Lambda Function uses the Kinesis as an Event Source. The system automatically scales when the stream contains image events.
D. Create an Auto Scaling, Load Balanced Elastic Beanstalk worker tier Application and Environment. Deploy the ANN code to G2 instances in this tier. Set the desired capacity to 1. Make the code periodically check S3 for new manifests.When a new manifest is detected, push all of the images in the manifest into the SQS queue associated with the Elastic Beanstalk worker tier.

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

**Explanation/Reference:**
The Elastic Beanstalk option is incorrect because it requires a constantly-polling instance, which may break and costs money. The Lambda fleet option is incorrect because AWS Lambda does not support GPU usage. The OpsWorks stack option both requires a constantly-polling instance, and also requires

complex timing and capacity planning logic. The CloudFormation option requires no polling, has no always-on instances, and allows arbitrarily fast processing by simply setting the instance count as high as needed.
Reference: http://docs.aws.amazon.com/lambda/latest/dg/current-supported-versions.html

**QUESTION 344**
You are designing a system which needs, at minumum, 8 m4.large instances operating to service traffic. When designing a system for high availability in the us-east-1 region, which has 6 Availability Zones, you company needs to be able to handle death of a full availability zone. How should you distribute the servers, to save as much cost as possible, assuming all of the EC2 nodes are properly linked to an ELB?
Your VPC account can utilize us-east-1's AZ's a through f, inclusive.

A. 3 servers in each of AZ's a through d, inclusive.
B. 8 servers in each of AZ's a and b.
C. 2 servers in each of AZ's a through e, inclusive.
D. 4 servers in each of AZ's a through c, inclusive.

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

**Explanation/Reference:**
You need to design for N+1 redundancy on Availability Zones. ZONE_COUNT = (REQUIRED_INSTANCES / INSTANCE_COUNT_PER_ZONE) + 1. To minimize cost, spread the instances across as many possible zones as you can. By using a though e, you are allocating 5 zones. Using 2 instances, you have 10 total instances. If a single zone fails, you have 4 zones left, with 2 instances each, for a total of 8 instances. By spreading out as much as possible, you have increased cost by only 25% and significantly de-risked an availability zone failure.
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

**QUESTION 345**
You need to create a Route53 record automatically in CloudFormation when not running in production during all launches of a Template. How should you implement this?

A. Use a <code>Parameter</code> for <code>environment</code>, and add a <code>Condition</code> on the Route53 <code>Resource</code> in the template to create the record only when <code>environment</code> is not<code>production</code>.
B. Create two templates, one with the Route53 record value and one with a null value for the record. Use the one without it when deploying to production.
C. Use a <code>Parameter</code> for <code>environment</code>, and add a <code>Condition</code> on the Route53 <code>Resource</code> in the template to create the record with a null string when <code>environment</code> is<code>production</code>.
D. Create two templates, one with the Route53 record and one without it. Use the one without it when deploying to production.

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

**Explanation**

**Explanation/Reference:**
The best way to do this is with one template, and a Condition on the resource. Route53 does not allow null strings for records.
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/conditions-sectionstructure.html

**QUESTION 346**
What is web identity federation?

A. Use of an identity provider like Google or Facebook to become an AWS IAM User.
B. Use of an identity provider like Google or Facebook to exchange for temporary AWS security credentials.
C. Use of AWS IAM User tokens to log in as a Google or Facebook user.
D. Use of AWS STS Tokens to log in as a Google or Facebook user.

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

**Explanation/Reference:**
Users of your app can sign in using a well-known identity provider (IdP) - such as Login with Amazon, Facebook, Google, or any other OpenID Connect (OIDC)-compatible IdP, receive an authentication token, and then exchange that token for temporary security credentials in AWS that map to an IAM role with permissions to use the resources in your AWS account.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

**QUESTION 347**
You have been asked to de-risk deployments at your company. Specifically, the CEO is concerned about outages that occur because of accidental inconsistencies between Staging and Production, which sometimes cause unexpected behaviors in Production even when Staging tests pass. You already use Docker to get high consistency between Staging and Production for the application environment on your EC2 instances.
How do you further de-risk the rest of the execution environment, since in AWS, there are many service components you may use beyond EC2 virtual machines?

A. Develop models of your entire cloud system in CloudFormation. Use this model in Staging and Production to achieve greater parity.
B. Use AWS Config to force the Staging and Production stacks to have configuration parity. Any differences will be detected for you so you are aware of risks.
C. Use AMIs to ensure the whole machine, including the kernel of the virual machines, is consistent, since Docker uses Linux Container (LXC) technology, and we need to make sure the container environment is consistent.
D. Use AWS ECS and Docker clustering. This will make sure that the AMIs and machine sizes are the same across both environments.

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

**Explanation**

**Explanation/Reference:**
Only CloudFormation's JSON Templates allow declarative version control of repeatably deployable models of entire AWS clouds.
Reference: https://blogs.aws.amazon.com/application-management/blog/category/Best+practices

**QUESTION 348**
You are creating a new API for video game scores. Reads are 100 times more common than writes, and the top 1% of scores are read 100 times more frequently than the rest of the scores. What's the best design for this system, using DynamoDB?

A. DynamoDB table with 100x higher read than write throughput, with CloudFront caching.
B. DynamoDB table with roughly equal read and write throughput, with CloudFront caching.
C. DynamoDB table with 100x higher read than write throughput, with ElastiCache caching.
D. DynamoDB table with roughly equal read and write throughput, with ElastiCache caching.

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

**Explanation/Reference:**
Because the 100x read ratio is mostly driven by a small subset, with caching, only a roughly equal number of reads to writes will miss the cache, since the supermajority will hit the top 1% scores. Knowing we need to set the values roughly equal when using caching, we select AWS ElastiCache, because CloudFront cannot directly cache DynamoDB queries, and ElastiCache is an excellent in-memory cache for database queries, rather than a distributed proxy cache for content delivery. ... One solution would be to cache these reads at the application layer. Caching is a technique that is used in many high-throughput applications, offloading read activity on hot items to the cache rather than to the database.
Your application can cache the most popular items in memory, or use a product such as ElastiCache to do the same.
Reference:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/best-practices.html#%20Guideli%20nesForTables.CachePopularItem

**QUESTION 349**
You were just hired as a DevOps Engineer for a startup. Your startup uses AWS for 100% of their infrastructure. They currently have no automation at all for deployment, and they have had many failures while trying to deploy to production. The company has told you deployment process risk mitigation is the most important thing now, and you have a lot of budget for tools and AWS resources. Their stack:

```
2-tier API
Data stored in DynamoDB or S3, depending on type
Compute layer is EC2 in Auto Scaling Groups
They use Route53 for DNS pointing to an ELB
An ELB balances load across the EC2 instances
```

The scaling group properly varies between 4 and 12 EC2 servers.
Which of the following approaches, given this company's stack and their priorities, best meets the company's needs?

A. Model the stack in AWS Elastic Beanstalk as a single Application with multiple Environments. Use Elastic Beanstalk's Rolling Deploy option to progressively roll out application code changes when promoting across environments.
B. Model the stack in 3 CloudFormation templates: Data layer, compute layer, and networking layer. Write stack deployment and integration testing automation following Blue-Green methodologies.
C. Model the stack in AWS OpsWorks as a single Stack, with 1 compute layer and its associated ELB. Use Chef and App Deployments to automate Rolling Deployment.
D. Model the stack in 1 CloudFormation template, to ensure consistency and dependency graph resolution. Write deployment and integration testing automation following Rolling Deployment methodologies.



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

**Explanation/Reference:**
AWS recommends Blue-Green for zero-downtime deploys. Since you use DynamoDB, and neither AWS OpsWorks nor AWS Elastic Beanstalk directly supports DynamoDB, the option selecting CloudFormation and Blue-Green is correct.
You use various strategies to migrate the traffic from your current application stack (blue) to a new version of the application (green). This is a popular technique for deploying applications with zero downtime. The deployment services like AWS Elastic Beanstalk, AWS CloudFormation, or AWS OpsWorks are particularly useful as they provide a simple way to clone your running application stack. You can set up a new version of your application (green) by simply cloning current version of the application (blue).

**QUESTION 350**
What is the scope of an EBS snapshot?

A. Availability Zone
B. Placement Group
C. Region
D. VPC

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

**Explanation/Reference:**
Section: (none)

An EBS snapshot is tied to its region and can only be used to create volumes in the same region. You can copy a snapshot from one region to another. For more information, see Copying an Amazon EBS Snapshot.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

**QUESTION 351**
Your system uses a multi-master, multi-region DynamoDB configuration spanning two regions to achieve high availablity. For the first time since launching your system, one of the AWS Regions in which you operate over went down for 3 hours, and the failover worked correctly. However, after recovery, your users are experiencing strange bugs, in which users on different sides of the globe see different data. What is a likely design issue that was not accounted for when launching?

A. The system does not have Lambda Functor Repair Automatons, to perform table scans and chack for corrupted partition blocks inside the Table in the recovered Region.
B. The system did not implement DynamoDB Table Defragmentation for restoring partition performance in the Region that experienced an outage, so data is served stale.
C. The system did not include repair logic and request replay buffering logic for post-failure, to resynchronize data to the Region that was unavailable for a number of hours.
D. The system did not use DynamoDB Consistent Read requests, so the requests in different areas are not utilizing consensus across Regions at runtime.

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

**Explanation/Reference:**
When using multi-region DynamoDB systems, it is of paramount importance to make sure that all requests made to one Region are replicated to the other. Under normal operation, the system in question-would correctly perform write replays into the other Region. If a whole Region went down, the system would be unable to perform these writes for the period of downtime. Without buffering write requests somehow, there would be no way for the system to replay dropped crossregion writes, and the requests would be serviced differently depending on the Region from which they were served after recovery.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.CrossRegionRepl.html

**QUESTION 352**

There are a number of ways to purchase compute capacity on AWS. Which orders the price per compute or memory unit from LOW to HIGH (cheapest to most expensive), on average?
A - On-Demand
B - Spot
C - Reserved

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

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

**Explanation/Reference:**
Spot instances are usually many, many times cheaper than on-demand prices. Reserved instances, depending on their term and utilization, can yield approximately 33% to 66% cost savings. On-Demand prices are the baseline price and are the most expensive way to purchase EC2 compute time.
Reference: https://d0.awsstatic.com/whitepapers/Cost_Optimization_with_AWS.pdf



**QUESTION 353**
You run operations for a company that processes digital wallet payments at a very high volume. One second of downtime, during which you drop payments or are otherwise unavailable, loses you on average USD 100. You balance the financials of the transaction system once per day.
Which database setup is best suited to address this business risk?

A. A multi-AZ RDS deployment with synchronous replication to multiple standbys and read-replicas for fast failover and ACID properties.
B. A multi-region, multi-master, active-active RDS configuration using database-level ACID design principles with database trigger writes for replication.
C. A multi-region, multi-master, active-active DynamoDB configuration using application control-level BASE design principles with change-stream write queue buffers for replication.
D. A multi-AZ DynamoDB setup with changes streamed to S3 via AWS Kinesis, for highly durable storage and BASE properties.

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

**Explanation/Reference:**
Only the multi-master, multi-region DynamoDB answer makes sense. Multi-AZ deployments do not provide sufficient availability when a business loses USD 360,000 per hour of unavailability. As RDS does not natively support multi-region, and ACID does not perform well/at all over large distances between regions, only the DynamoDB answer works.

Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.CrossRegionRepl.html

**QUESTION 354**
When thinking of DynamoDB, what are true of Local Secondary Key properties?

A. Either the partition key or the sort key can be different from the table, but not both.
B. Only the sort key can be different from the table.
C. The partition key and sort key can be different from the table.
D. Only the partition key can be different from the table.

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

**Explanation/Reference:**
Global secondary index - an index with a partition key and a sort key that can be different from those on the table. A global secondary index is considered "global" because queries on the index can span all of the data in a table, across all partitions.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html

**QUESTION 355**
Which deployment method, when using AWS Auto Scaling Groups and Auto Scaling Launch Configurations, enables the shortest time to live for individual servers?

A. Pre-baking AMIs with all code and configuration on deploys.
B. Using a Dockerfile bootstrap on instance launch.
C. Using UserData bootstrapping scripts.
D. Using AWS EC2 Run Commands to dynamically SSH into fleets.

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

**Explanation/Reference:**
Note that the bootstrapping process can be slower if you have a complex application or multiple applications to install. Managing a fleet of applications with several build tools and dependencies can be a challenging task during rollouts. Furthermore, your deployment service should be designed to do faster rollouts to take advantage of Auto Scaling. Prebaking is a process of embedding a significant portion of your application artifacts within your base AMI. During the deployment process you can customize application installations by using EC2 instance artifacts such as instance tags, instance metadata, and Auto Scaling groups.
Reference:

https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf

**QUESTION 356**
Which of these techniques enables the fastest possible rollback times in the event of a failed deployment?

A. Rolling; Immutable
B. Rolling; Mutable
C. Canary or A/B
D. Blue-Green

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

**Explanation/Reference:**
AWS specifically recommends Blue-Green for super-fast, zero-downtime deploys - and thus rollbacks, which are redeploying old code. You use various strategies to migrate the traffic from your current application stack (blue) to a new version of the application (green). This is a popular technique for deploying applications with zero downtime.
Reference: https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-onaws.pdf



**QUESTION 357**
Which of the following are not valid sources for OpsWorks custom cookbook repositories?

A. HTTP(S)
B. Git
C. AWS EBS
D. Subversion

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

**Explanation/Reference:**
Linux stacks can install custom cookbooks from any of the following repository types: HTTP or Amazon S3 archives. They can be either public or private, but Amazon S3 is typically the preferred option for a private archive. Git and Subversion repositories provide source control and the ability to have multiple versions.
Reference:
http://docs.aws.amazon.com/opsworks/latest/userguide/workingcookbook-installingcustomenable.html

**QUESTION 358**

You are building a deployment system on AWS. You will deploy new code by bootstrapping instances in a private subnet in a VPC at runtime using UserData scripts pointing to an S3 zip file object, where your code is stored. An ELB in a public subnet has network interfaces and connectivity to the instances. Requests from users of the system are routed to the ELB via a Route53 A Record Alias. You do not use any VPC endpoints. Which is a risk of using this approach?

A. Route53 Alias records do not always update dynamically with ELB network changes after deploys.
B. If the NAT routing for the private subnet fails, deployments fail.
C. Kernel changes to the base AMI may render the code inoperable.
D. The instances cannot be in a private subnet if the ELB is in a public one.

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

**Explanation/Reference:**
Since you are not using VPC endpoints, outbound requests for the code sitting in S3 are routed though the NAT for the VPC's private subnets. If this networking fails, runtime bootstrapping through code download will fail due to network unavailability and lack of access to the Internet, and thus Amazon S3.
Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

**QUESTION 359**
Which major database needs a BYO license?



A. PostgreSQL
B. MariaDB
C. MySQL
D. Oracle

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

**Explanation/Reference:**
Oracle is not open source, and requires a bring your own license model.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Oracle.html

**QUESTION 360**
What is the maximum supported single-volume throughput on EBS?

A. 320MiB/s
B. 160MiB/s

C. 40MiB/s
D. 640MiB/s

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

**Explanation/Reference:**
The ceiling throughput for PIOPS on EBS is 320MiB/s.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

**QUESTION 361**
When a user is detaching an EBS volume from a running instance and attaching it to a new instance, which of the below mentioned options should be followed to avoid file system damage?

A. Unmount the volume first
B. Stop all the I/O of the volume before processing
C. Take a snapshot of the volume before detaching
D. Force Detach the volume to ensure that all the data stays intact



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

**Explanation/Reference:**
When a user is trying to detach an EBS volume, the user can either terminate the instance or explicitly remove the volume. It is a recommended practice to unmount the volume first to avoid any file system damage.

**QUESTION 362**
A user is creating a new EBS volume from an existing snapshot. The snapshot size shows 10 GB. Can the user create a volume of 30 GB from that snapshot?

A. Provided the original volume has set the change size attribute to true
B. Yes
C. Provided the snapshot has the modify size attribute set as true
D. No

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

**Explanation/Reference:**
Section: (none)

A user can always create a new EBS volume of a higher size than the original snapshot size. The user cannot create a volume of a lower size. When the new volume is created the size in the instance will be shown as the original size. The user needs to change the size of the device with resize2fs or other OS specific commands.

**QUESTION 363**
How long are the messages kept on an SQS queue by default?

A. If a message is not read, it is never deleted
B. 2 weeks
C. 1 day
D. 4 days

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



**Explanation/Reference:**
The SQS message retention period is configurable and can be set anywhere from 1 minute to 2 weeks. The default is 4 days and once the message retention limit is reached your messages will be automatically deleted. The option for longer message retention provides greater flexibility to allow for longer intervals between message production and consumption.

**QUESTION 364**
A user has attached an EBS volume to a running Linux instance as a "/dev/sdf" device. The user is unable to see the attached device when he runs the command "df -h". What is the possible reason for this?

A. The volume is not in the same AZ of the instance
B. The volume is not formatted
C. The volume is not attached as a root device
D. The volume is not mounted

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

**Explanation/Reference:**
When a user creates an EBS volume and attaches it as a device, it is required to mount the device. If the device/volume is not mounted it will not be available in the listing.

**QUESTION 365**
When using Amazon SQS how much data can you store in a message?

A. 8 KB
B. 2 KB
C. 16 KB
D. 4 KB

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

**Explanation/Reference:**
With Amazon SQS version 2008-01-01, the maximum message size for both SOAP and Query requests is 8KB. If you need to send messages to the queue that are larger than 8 KB, AWS recommends that you split the information into separate messages. Alternatively, you could use Amazon S3 or Amazon SimpleDB to hold the information and include the pointer to that information in the Amazon SQS message. If you send a message that is larger than 8KB to the queue, you will receive a MessageTooLong error with HTTP code 400.

**QUESTION 366**
What is the maximum time messages can be stored in SQS?

A. 14 days
B. one month
C. 4 days
D. 7 days

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

**Explanation/Reference:**
A message can be stored in the Simple Queue Service (SQS) from 1 minute up to a maximum of 14 days.

**QUESTION 367**

In DynamoDB, a secondary index is a data structure that contains a subset of attributes from a table, along with an alternate key to support _____ operations.

A. None of the above
B. Both
C. Query
D. Scan

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

**Explanation/Reference:**
In DynamoDB, a secondary index is a data structure that contains a subset of attributes from a table, along with an alternate key to support Query operations.

**QUESTION 368**
A user has created a new EBS volume from an existing snapshot. The user mounts the volume on the instance to which it is attached. Which of the below mentioned options is a required step before the user can mount the volume?

A. Run a cyclic check on the device for data consistency
B. Create the file system of the volume
C. Resize the volume as per the original snapshot size
D. No step is required. The user can directly mount the device



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

**Explanation/Reference:**
When a user is trying to mount a blank EBS volume, it is required that the user first creates a file system within the volume. If the volume is created from an existing snapshot then the user needs not to create a file system on the volume as it will wipe out the existing data.

**QUESTION 369**
You need your CI to build AMIs with code pre-installed on the images on every new code push. You need to do this as cheaply as possible. How do you do this?

A. Bid on spot instances just above the asking price as soon as new commits come in, perform all instance configuration and setup, then create an AMI based on the spot instance.
B. Have the CI launch a new on-demand EC2 instance when new commits come in, perform all instance configuration and setup, then create an AMI based on the on-demand instance.
C. Purchase a Light Utilization Reserved Instance to save money on the continuous integration machine. Use these credits whenever your create AMIs on

instances.

D. When the CI instance receives commits, attach a new EBS volume to the CI machine. Perform all setup on this EBS volume so you do not need a new EC2 instance to create the AMI.

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

**Explanation/Reference:**
Spot instances are the cheapest option, and you can use minimum run duration if your AMI takes more than a few minutes to create. Spot instances are also available to run for a predefined duration - in hourly increments up to six hours in length - at a significant discount (30-45%) compared to On-Demand pricing plus an additional 5% during off-peak times1 for a total of up to 50% savings.
Reference:
https://aws.amazon.com/ec2/spot/pricing/

**QUESTION 370**
When thinking of DynamoDB, what are true of Global Secondary Key properties?

A. The partition key and sort key can be different from the table.
B. Only the partition key can be different from the table.
C. Either the partition key or the sort key can be different from the table, but not both.
D. Only the sort key can be different from the table.



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

**Explanation/Reference:**
Global secondary index - an index with a partition key and a sort key that can be different from those on the table. A global secondary index is considered "global" because queries on the index can span all of the data in a table, across all partitions.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SecondaryIndexes.html

**QUESTION 371**
You need to process long-running jobs once and only once. How might you do this?

A. Use an SNS queue and set the visibility timeout to long enough for jobs to process.
B. Use an SQS queue and set the reprocessing timeout to long enough for jobs to process.
C. Use an SQS queue and set the visibility timeout to long enough for jobs to process.
D. Use an SNS queue and set the reprocessing timeout to long enough for jobs to process.

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

**Explanation/Reference:**
The message timeout defines how long after a successful receive request SQS waits before allowing jobs to be seen by other components, and proper configuration prevents duplicate processing.
Reference: http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/MessageLife cycle.html

**QUESTION 372**
You are getting a lot of empty receive requests when using Amazon SQS. This is making a lot of unnecessary network load on your instances. What can you do to reduce this load?

A. Subscribe your queue to an SNS topic instead.
B. Use as long of a poll as possible, instead of short polls.
C. Alter your visibility timeout to be shorter.
D. Use <code>sqsd</code> on your EC2 instances.



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

**Explanation/Reference:**
Section: (none)

One benefit of long polling with Amazon SQS is the reduction of the number of empty responses, when there are no messages available to return, in reply to a ReceiveMessage request sent to an Amazon SQS queue. Long polling allows the Amazon SQS service to wait until a message is available in the queue before sending a response.
Reference:
http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-longpolling.html

**QUESTION 373**
You need to know when you spend $1000 or more on AWS. What's the easy way for you to see that notification?

A. AWS CloudWatch Events tied to API calls, when certain thresholds are exceeded, publish to SNS.
B. Scrape the billing page periodically and pump into Kinesis.

C. AWS CloudWatch Metrics + Billing Alarm + Lambda event subscription. When a threshold is exceeded, email the manager.
D. Scrape the billing page periodically and publish to SNS.

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

**Explanation/Reference:**
Even if you're careful to stay within the free tier, it's a good idea to create a billing alarm to notify you if you exceed the limits of the free tier. Billing alarms can help to protect you against unknowingly accruing charges if you inadvertently use a service outside of the free tier or if traffic exceeds your expectations.
Reference:
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/freetier-alarms.html

**QUESTION 374**
You need to grant a vendor access to your AWS account. They need to be able to read protected messages in a private S3 bucket at their leisure. They also use AWS. What is the best way to accomplish this?

A. Create an IAM User with API Access Keys. Grant the User permissions to access the bucket. Give the vendor the AWS Access Key ID and AWS Secret Access Key for the User.
B. Create an EC2 Instance Profile on your account. Grant the associated IAM role full access to the bucket. Start an EC2 instance with this Profile and give SSH access to the instance to the vendor.
C. Create a cross-account IAM Role with permission to access the bucket, and grant permission to use the Role to the vendor AWS account.
D. Generate a signed S3 PUT URL and a signed S3 PUT URL, both with wildcard values and 2 year durations. Pass the URLs to the vendor.

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

**Explanation/Reference:**
When third parties require access to your organization's AWS resources, you can use roles to delegate access to them. For example, a third party might provide a service for managing your AWS resources. With IAM roles, you can grant these third parties access to your AWS resources without sharing your AWS security credentials. Instead, the third party can access your AWS resources by assuming a role that you create in your AWS account.
Reference:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

**QUESTION 375**
Your serverless architecture using AWS API Gateway, AWS Lambda, and AWS DynamoDB experienced a large increase in traffic to a sustained 400 requests per second, and dramatically increased in failure rates. Your requests, during normal operation, last 500 milliseconds on average. Your DynamoDB table did not exceed 50% of provisioned throughput, and Table primary keys are designed correctly. What is the most likely issue?

A. Your API Gateway deployment is throttling your requests.
B. Your AWS API Gateway Deployment is bottlenecking on request (de)serialization.
C. You did not request a limit increase on concurrent Lambda function executions.
D. You used Consistent Read requests on DynamoDB and are experiencing semaphore lock.

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

**Explanation/Reference:**
Section: (none)

AWS API Gateway by default throttles at 500 requests per second steady-state, and 1000 requests per second at spike. Lambda, by default, throttles at 100 concurrent requests for safety. At 500 milliseconds (half of a second) per request, you can expect to support 200 requests per second at 100 concurrency. This is less than the 400 requests per second your system now requires. Make a limit increase request via the AWS Support Console. AWS Lambda: Concurrent requests safety throttle per account -> 100.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_lambda



**QUESTION 376**
Why are more frequent snapshots or EBS Volumes faster?

A. Blocks in EBS Volumes are allocated lazily, since while logically separated from other EBS Volumes, Volumes often share the same physical hardware. Snapshotting the first time forces full block range allocation, so the second snapshotdoesn't need to perform the allocation phase and is faster.
B. The snapshots are incremental so that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot.
C. AWS provisions more disk throughput for burst capacity during snapshots if the drive has been pre-warmed by snapshotting and reading all blocks.
D. The drive is pre-warmed, so block access is more rapid for volumes when every block on the device has already been read at least one time.

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

**Explanation/Reference:**
After writing data to an EBS volume, you can periodically create a snapshot of the volume to use as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental so that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the volume.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-snapshot.html

**QUESTION 377**
For AWS CloudFormation, which stack state refuses UpdateStack calls?

A. <code>UPDATE_ROLLBACK_FAILED</code>
B. <code>UPDATE_ROLLBACK_COMPLETE</code>
C. <code>UPDATE_COMPLETE</code>
D. <code>CREATE_COMPLETE</code>

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

**Explanation/Reference:**
When a stack is in the UPDATE_ROLLBACK_FAILED state, you can continue rolling it back to return it to a working state (to UPDATE_ROLLBACK_COMPLETE). You cannot update a stack that is in the UPDATE_ROLLBACK_FAILED state. However, if you can continue to roll it back, you can return the stack to its original settings and try to update it again.
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stackscontinueu pdaterollback.html

**QUESTION 378**
You need to migrate 10 million records in one hour into DynamoDB. All records are 1.5KB in size. The data is evenly distributed across the partition key. How many write capacity units should you provision during this batch load?

A. 6667
B. 4166
C. 5556
D. 2778

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

**Explanation/Reference:**
You need 2 units to make a 1.5KB write, since you round up. You need 20 million total units to perform this load. You have 3600 seconds to do so. Divide and round up for 5556.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ProvisionedT hroughput.html

**QUESTION 379**

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

A. Use CloudTrail Log File Integrity Validation.
B. Use AWS Config SNS Subscriptions and process events in real time.
C. Use CloudTrail backed up to AWS S3 and Glacier.
D. Use AWS Config Timeline forensics.

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

**Explanation/Reference:**
You must use CloudTrail Log File Validation (default or custom implementation), as any other tracking method is subject to forgery in the event of a full account compromise by sophisticated enough hackers. Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html



**QUESTION 380**
Which of these is not a Pseudo Parameter in AWS CloudFormation?

A. AWS::StackName
B. AWS::AccountId
C. AWS::StackArn
D. AWS::NotificationARNs

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

**Explanation/Reference:**
This is the complete list of Pseudo Parameters: AWS::AccountId, AWS::NotificationARNs, AWS::NoValue, AWS::Region, AWS::StackId, AWS::StackName.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/pseudo-parameterreference.html

**QUESTION 381**

What is the scope of an EBS volume?

A. VPC
B. Region
C. Placement Group
D. Availability Zone

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

**Explanation/Reference:**
An Amazon EBS volume is tied to its Availability Zone and can be attached only to instances in the same Availability Zone.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

**QUESTION 382**
You are experiencing performance issues writing to a DynamoDB table. Your system tracks high scores for video games on a marketplace. Your most popular game experiences all of the performance issues. What is the most likely problem?

A. DynamoDB's vector clock is out of sync, because of the rapid growth in request for the most popular game.
B. You selected the Game ID or equivalent identifier as the primary partition key for the table.
C. Users of the most popular video game each perform more read and write requests than average.
D. You did not provision enough read or write throughput to the table.

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

**Explanation/Reference:**
The primary key selection dramatically affects performance consistency when reading or writing to DynamoDB. By selecting a key that is tied to the identity of the game, you forced DynamoDB to create a hotspot in the table partitions, and over-request against the primary key partition for the popular game. When it stores data, DynamoDB divides a table's items into multiple partitions, and distributes the data primarily based upon the partition key value. The provisioned throughput associated with a table is also divided evenly among the partitions, with no sharing of provisioned throughput across partitions.

**QUESTION 383**
You meet once per month with your operations team to review the past month's data. During the meeting, you realize that 3 weeks ago, your monitoring system which pings over HTTP from outside AWS recorded a large spike in latency on your 3-tier web service API. You use DynamoDB for the database layer, ELB, EBS, and EC2 for the business logic tier, and SQS, ELB, and EC2 for the presentation layer. Which of the following techniques will NOT help you figure out what happened?

A. Check your CloudTrail log history around the spike's time for any API calls that caused slowness.
B. Review CloudWatch Metrics graphs to determine which component(s) slowed the system down.
C. Review your ELB access logs in S3 to see if any ELBs in your system saw the latency.
D. Analyze your logs to detect bursts in traffic at that time.

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

**Explanation/Reference:**
Metrics data are available for 2 weeks. If you want to store metrics data beyond that duration, you can retrieve it using our GetMetricStatistics API as well as a number of applications and tools offered by AWS partners.
Reference: https://aws.amazon.com/cloudwatch/faqs/

**QUESTION 384**
Which of these is not an intrinsic function in AWS CloudFormation?



A. Fn::Split
B. Fn::FindInMap
C. Fn::Select
D. Fn::GetAZs

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

**Explanation/Reference:**
This is the complete list of Intrinsic Functions...: Fn::Base64, Fn::And, Fn::Equals, Fn::If, Fn::Not, Fn::Or, Fn::FindInMap, Fn::GetAtt, Fn::GetAZs, Fn::Join, Fn::Select
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-functionreference.html

**QUESTION 385**
For AWS CloudFormation, which is true?

A. Custom resources using SNS have a default timeout of 3 minutes.
B. Custom resources using SNS do not need a <code>ServiceToken</code> property.
C. Custom resources using Lambda and <code>Code.ZipFile</code> allow inline nodejs resource composition.

D. Custom resources using Lambda do not need a <code>ServiceToken</code>property

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

**Explanation/Reference:**
Code is a property of the AWS::Lambda::Function resource that enables to you specify the source code of an AWS Lambda (Lambda) function. You can point to a file in an Amazon Simple Storage Service (Amazon S3) bucket or specify your source code as inline text (for nodejs runtime environments only).
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-customresources.html

**QUESTION 386**
Your API requires the ability to stay online during AWS regional failures. Your API does not store any state, it only aggregates data from other sources - you do not have a database. What is a simple but effective way to achieve this uptime goal?

A. Use a CloudFront distribution to serve up your API. Even if the region your API is in goes down, the edge locations CloudFront uses will be fine.
B. Use an ELB and a cross-zone ELB deployment to create redundancy across datacenters. Even if a region fails, the other AZ will stay online.
C. Create a Route53 Weighted Round Robin record, and if one region goes down, have that region redirect to the other region.
D. Create a Route53 Latency Based Routing Record with Failover and point it to two identical deployments of your stateless API in two different regions. Make sure both regions use Auto Scaling Groups behind ELBs.



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

**Explanation/Reference:**
Latency Based Records allow request distribution when all is well with both regions, and the Failover component enables fallbacks between regions. By adding in the ELB and ASG, your system in the surviving region can expand to meet 100% of demand instead of the original fraction, whenever failover occurs.
Reference: http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html

**QUESTION 387**
You are designing an enterprise data storage system. Your data management software system requires mountable disks and a real filesystem, so you cannot use S3 for storage. You need persistence, so you will be using AWS EBS Volumes for your system. The system needs as lowcost storage as possible, and access is not frequent or high throughput, and is mostly sequential reads. Which is the most appropriate EBS Volume Type for this scenario?

A. gp1
B. io1
C. standard

D. gp2

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

**Explanation/Reference:**
Standard volumes, or Magnetic volumes, are best for: Cold workloads where data is infrequently accessed, or scenarios where the lowest storage cost is important.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

**QUESTION 388**
You need to deploy an AWS stack in a repeatable manner across multiple environments. You have selected CloudFormation as the right tool to accomplish this, but have found that there is a resource type you need to create and model, but is unsupported by CloudFormation. How should you overcome this challenge?

A. Use a CloudFormation Custom Resource Template by selecting an API call to proxy for create, update, and delete actions. CloudFormation will use the AWS SDK, CLI, or API method of your choosing as the state transition function forthe resource type you are modeling.
B. Submit a ticket to the AWS Forums. AWS extends CloudFormation Resource Types by releasing tooling to the AWS Labs organization on GitHub. Their response time is usually 1 day, and they complete requests within a week or two.
C. Instead of depending on CloudFormation, use Chef, Puppet, or Ansible to author Heat templates, which are declarative stack resource definitions that operate over the OpenStack hypervisor and cloud environment.
D. Create a CloudFormation Custom Resource Type by implementing create, update, and delete functionality, either by subscribing a Custom Resource Provider to an SNS topic, or by implementing the logic in AWS Lambda.

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

**Explanation/Reference:**
Custom resources provide a way for you to write custom provisioning logic in AWS CloudFormation template and have AWS CloudFormation run it during a stack operation, such as when you create, update or delete a stack. For more information, see Custom Resources.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-customresources.html

**QUESTION 389**
You run a 2000-engineer organization. You are about to begin using AWS at a large scale for the first time. You want to integrate with your existing identity management system running on Microsoft Active Directory, because your organization is a power-user of Active Directory. How should you manage your AWS identities in the most simple manner?

A. Use a large AWS Directory Service Simple AD.

B. Use a large AWS Directory Service AD Connector.
C. Use an Sync Domain running on AWS Directory Service.
D. Use an AWS Directory Sync Domain running on AWS Lambda

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

**Explanation/Reference:**
You must use AD Connector as a power-user of Microsoft Active Directory. Simple AD only works with a subset of AD functionality. Sync Domains do not exist; they are made up answers. AD Connector is a directory gateway that allows you to proxy directory requests to your on-premises Microsoft Active Directory, without caching any information in the cloud. AD Connector comes in 2 sizes; small and large. A small AD Connector is designed for smaller organizations of up to 500 users. A large AD Connector is designed for larger organizations of up to 5,000 users.
Reference:
https://aws.amazon.com/directoryservice/details/

**QUESTION 390**
When thinking of AWS OpsWorks, which of the following is not an instance type you can allocate in a stack layer?



A. 24/7 instances
B. Spot instances
C. Time-based instances
D. Load-based instances

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

**Explanation/Reference:**
AWS OpsWorks supports the following instance types, which are characterized by how they are started and stopped. 24/7 instances are started manually and run until you stop them.Time-based instances are run by AWS
OpsWorks on a specified daily and weekly schedule. They allow your stack to automatically adjust the number of instances to accommodate predictable usage patterns. Load-based instances are automatically started and stopped by AWS OpsWorks, based on specified load metrics, such as CPU utilization. They allow your stack to automatically adjust the number of instances to accommodate variations in incoming traffic. Load-based instances are available only for Linuxbased stacks.
Reference: http://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html

**QUESTION 391**
Which of these is not a CloudFormation Helper Script?

A. cfn-signal
B. cfn-hup
C. cfn-request
D. cfn-get-metadata

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

**Explanation/Reference:**
This is the complete list of CloudFormation Helper Scripts: cfn-init, cfn-signal, cfn-get-metadata, cfn-hup
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-helper-scriptsreference.html

**QUESTION 392**
Your team wants to begin practicing continuous delivery using CloudFormation, to enable automated builds and deploys of whole, versioned stacks or stack layers. You have a 3-tier, mission-critical system. Which of the following is NOT a best practice for using CloudFormation in a continuous delivery environment?

A. Use the AWS CloudFormation <code>ValidateTemplate</code> call before publishing changes to AWS.
B. Model your stack in one template, so you can leverage CloudFormation's state management and dependency resolution to propagate all changes.
C. Use CloudFormation to create brand new infrastructure for all stateless resources on each push, and run integration tests on that set of infrastructure.
D. Parametrize the template and use <code>Mappings</code> to ensure your template works in multiple Regions.

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

**Explanation/Reference:**
Putting all resources in one stack is a bad idea, since different tiers have different life cycles and frequencies of change. For additional guidance about organizing your stacks, you can use two common frameworks: a multi-layered architecture and service-oriented architecture (SOA).
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/bestpractices.html#organizingstacks

**QUESTION 393**
You need to replicate API calls across two systems in real time. What tool should you use as a buffer and transport mechanism for API call events?

A. AWS SQS
B. AWS Lambda
C. AWS Kinesis

D. AWS SNS

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

**Explanation/Reference:**
AWS Kinesis is an event stream service. Streams can act as buffers and transport across systems for in-order programmatic events, making it ideal for replicating API calls across systems. A typical Amazon Kinesis Streams application reads data from an Amazon Kinesis stream as data records. These applications can use the Amazon Kinesis Client Library, and they can run on Amazon EC2 instances. The processed records can be sent to dashboards, used to generate alerts, dynamically change pricing and advertising strategies, or send data to a variety of other AWS services. For information about Streams features and pricing, see Amazon Kinesis Streams.
Reference:
http://docs.aws.amazon.com/kinesis/latest/dev/introduction.html

**QUESTION 394**
You are building a Ruby on Rails application for internal, non-production use which uses MySQL as a database. You want developers without very much AWS experience to be able to deploy new code with a single command line push. You also want to set this up as simply as possible. Which tool is ideal for this setup?



A. AWS CloudFormation
B. AWS OpsWorks
C. AWS ELB + EC2 with CLI Push
D. AWS Elastic Beanstalk

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

**Explanation/Reference:**
Elastic Beanstalk's primary mode of operation exactly supports this use case out of the box. It is simpler than all the other options for this question. With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.
Reference: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_Ruby_rails.html

**QUESTION 395**
What is the scope of AWS IAM?

A. Global
B. Availability Zone

C. Region
D. Placement Group

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

**Explanation/Reference:**
IAM resources are all global; there is not regional constraint.
Reference: https://aws.amazon.com/iam/faqs/

**QUESTION 396**
You are building a mobile app for consumers to post cat pictures online. You will be storing the images in AWS S3. You want to run the system very cheaply and simply.
Which one of these options allows you to build a photo sharing application without needing to worry about scaling expensive uploads processes, authentication/ authorization and so forth?

A. Build the application out using AWS Cognito and web identity federation to allow users to log in using Facebook or Google Accounts. Once they are logged in, the secret token passed to that user is used to directly access resources onAWS, like AWS S3.
B. Use JWT or SAML compliant systems to build authorization policies. Users log in with a username and password, and are given a token they can use indefinitely to make calls against the photo infrastructure.
C. Use AWS API Gateway with a constantly rotating API Key to allow access from the client-side. Construct a custom build of the SDK and include S3 access in it.
D. Create an AWS oAuth Service Domain ad grant public signup and access to the domain. During setup, add at least one major social media site as a trusted Identity Provider for users.

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

**Explanation/Reference:**
The short answer is that Amazon Cognito is a superset of the functionality provided by web identity federation. It supports the same providers, and you configure your app and authenticate with those providers in the same way. But Amazon Cognito includes a variety of additional features. For example, it enables your users to start using the app as a guest user and later sign in using one of the supported identity providers.
Reference:
https://blogs.aws.amazon.com/security/post/Tx3SYCORF5EKRC0/How-Does-Amazon-CognitoRelate-to-Existing-Web-Identity-Federatio

**QUESTION 397**
Your CTO has asked you to make sure that you know what all users of your AWS account are doing to change resources at all times. She wants a report of who is doing what over time, reported to her once per week, for as broad a resource type group as possible.

How should you do this?

A. Create a global AWS CloudTrail Trail. Configure a script to aggregate the log data delivered to S3 once per week and deliver this to the CTO.
B. Use CloudWatch Events Rules with an SNS topic subscribed to all AWS API calls. Subscribe the CTO to an email type delivery on this SNS Topic.
C. Use AWS IAM credential reports to deliver a CSV of all uses of IAM User Tokens over time to the CTO.
D. Use AWS Config with an SNS subscription on a Lambda, and insert these changes over time into a DynamoDB table. Generate reports based on the contents of this table.

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

**Explanation/Reference:**
This is the ideal use case for AWS CloudTrail. CloudTrail provides visibility into user activity by recording API calls made on your account. CloudTrail records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.
Reference:
https://aws.amazon.com/cloudtrail/faqs/



**QUESTION 398**
What is the order of most-to-least rapidly-scaling (fastest to scale first)?

a) EC2 + ELB + Auto Scaling
b) Lambda
c) RDS

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

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

**Explanation/Reference:**
Lambda is designed to scale instantly. EC2 + ELB + Auto Scaling require single-digit minutes to scale out. RDS will take at least 15 minutes, and will apply OS

patches or any other updates when applied.
Reference: https://aws.amazon.com/lambda/faqs/

**QUESTION 399**
Which is not a restriction on AWS EBS Snapshots?

A. Snapshots which are shared cannot be used as a basis for other snapshots.
B. You cannot share a snapshot containing an AWS Access Key ID or AWS Secret Access Key.
C. You cannot share unencrypted snapshots.
D. Snapshot restorations are restricted to the region in which the snapshots are created.

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

**Explanation/Reference:**
Snapshots shared with other users are usable in full by the recipient, including but limited to the ability to base modified volumes and snapshots.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshotpermissions.html

**QUESTION 400**
You need to deploy a new application version to production. Because the deployment is high-risk, you need to roll the new version out to users over a number of hours, to make sure everything is working correctly. You need to be able to control the proportion of users seeing the new version of the application down to the percentage point. You use ELB and EC2 with Auto Scaling Groups and custom AMIs with your code pre-installed assigned to Launch Configurations. There are no database-level changes during your deployment. You have been told you cannot spend too much money, so you must not increase the number of EC2 instances much at all during the deployment, but you also need to be able to switch back to the original version of code quickly if something goes wrong. What is the best way to meet these requirements?

A. Create a second ELB, Auto Scaling Launch Configuration, and Auto Scaling Group using the Launch Configuration. Create AMIs with all code pre-installed. Assign the new AMI to the second Auto Scaling Launch Configuration. UseRoute53 Weighted Round Robin Records to adjust the proportion of traffic hitting the two ELBs.
B. Use the Blue-Green deployment method to enable the fastest possible rollback if needed. Create a full second stack of instances and cut the DNS over to the new stack of instances, and change the DNS back if a rollback is needed.
C. Create AMIs with all code pre-installed. Assign the new AMI to the Auto Scaling Launch Configuration, to replace the old one. Gradually terminate instances running the old code (launched with the old Launch Configuration) and allow thenew AMIs to boot to adjust the traffic balance to the new code. On rollback, reverse the process by doing the same thing, but changing the AMI on the Launch Config back to the original code.
D. Migrate to use AWS Elastic Beanstalk. Use the established and well-tested Rolling Deployment setting AWS provides on the new Application Environment, publishing a zip bundle of the new code and adjusting the wait period to spreadthe deployment over time. Re-deploy the old code bundle to rollback if needed.

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

**Explanation/Reference:**
Only Weighted Round Robin DNS Records and reverse proxies allow such fine-grained tuning of traffic splits. The Blue-Green option does not meet the requirement that we mitigate costs and keep overall EC2 fleet size consistent, so we must select the 2 ELB and ASG option with WRR DNS tuning. This method is called A/B deployment and/or Canary deployment.
Reference:
https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf

**QUESTION 401**
What is required to achieve gigabit network throughput on EC2? You already selected cluster-compute, 10GB instances with enhanced networking, and your workload is already network-bound, but you are not seeing 10 gigabit speeds.

A. Enable biplex networking on your servers, so packets are non-blocking in both directions and there's no switching overhead.
B. Ensure the instances are in different VPCs so you don't saturate the Internet Gateway on any one VPC.
C. Select PIOPS for your drives and mount several, so you can provision sufficient disk throughput.
D. Use a placement group for your instances so the instances are physically near each other in the same Availability Zone.



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

**Explanation/Reference:**
You are not guaranteed 10gigabit performance, except within a placement group. A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a lowlatency, 10 Gbps network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

**QUESTION 402**
If you want CloudFormation stack status updates to show up in a continuous delivery system in as close to real time as possible, how should you achieve this?

A. Use a long-poll on the Resources object in your CloudFormation stack and display those state changes in the UI for the system.
B. Use a long-poll on the <code>ListStacksAPI</code> call for your CloudFormation stack and display those state changes in the UI for the system.
C. Subscribe your continuous delivery system to an SNS topic that you also tell your CloudFormation stack to publish events into.
D. Subscribe your continuous delivery system to an SQS queue that you also tell your CloudFormation stack to publish events into.

**Correct Answer:** C

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

**Explanation/Reference:**
Use NotificationARNs.member.N when making a CreateStack call to push stack events into SNS in nearly real-time.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacksmonitor-stack.html

**QUESTION 403**
What does it mean if you have zero IOPS and a non-empty I/O queue for all EBS volumes attached to a running EC2 instance?

A. The I/O queue is buffer flushing.
B. Your EBS disk head(s) is/are seeking magnetic stripes.
C. The EBS volume is unavailable.
D. You need to re-mount the EBS volume in the OS.

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



**Explanation/Reference:**
This is the definition of Unavailable from the EC2 and EBS SLA. "Unavailable" and "Unavailability" mean... For Amazon EBS, when all of your attached volumes perform zero read write IO, with pending IO in the queue.
Reference: https://aws.amazon.com/ec2/sla/

**QUESTION 404**
From a compliance and security perspective, which of these statements is true?

A. You do not ever need to rotate access keys for AWS IAM Users.
B. You do not ever need to rotate access keys for AWS IAM Roles, nor AWS IAM Users.
C. None of the other statements is true.
D. You do not ever need to rotate access keys for AWS IAM Roles.

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

**Explanation/Reference:**
IAM Role Access Keys are auto-rotated by AWS on your behalf; you do not need to rotate them. The application is granted the permissions for the actions and

resources that you have defined for the role through the security credentials associated with the role. These security credentials are temporary and we rotate them automatically. We make new credentials available at least five minutes prior to the expiration of the old credentials.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

**QUESTION 405**
Which of these configuration or deployment practices is a security risk for RDS?

A. Storing SQL function code in plaintext
B. Non-Multi-AZ RDS instance
C. Having RDS and EC2 instances exist in the same subnet
D. RDS in a public subnet

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

**Explanation/Reference:**
Making RDS accessible to the public internet in a public subnet poses a security risk, by making your database directly addressable and spammable. DB instances deployed within a VPC can be configured to be accessible from the Internet or from EC2 instances outside the VPC. If a VPC security group specifies a port access such as TCP port 22, you would not be able to access the DB instance because the firewall for the DB instance provides access only via the IP addresses specified by the DB security groups the instance is a member of and the port defined when the DB instance was created.
Reference:
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSSecurityGroups.html

**QUESTION 406**
Which of these is not a reason a Multi-AZ RDS instance will failover?

A. An Availability Zone outage
B. A manual failover of the DB instance was initiated using Reboot with failover
C. To autoscale to a higher instance class
D. The primary DB instance fails

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

**Explanation/Reference:**
The primary DB instance switches over automatically to the standby replica if any of the > following conditions occur: An Availability Zone outage, the primary DB instance fails, the DB instance's server type is changed, the operating system of the DB instance is, undergoing software patching, a manual failover of the

DB instance was initiated using Reboot with failover.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

**QUESTION 407**
You need to create an audit log of all changes to customer banking data. You use DynamoDB to store this customer banking data. It is important not to lose any information due to server failures. What is an elegant way to accomplish this?

A. Use a DynamoDB StreamSpecification and stream all changes to AWS Lambda. Log the changes to AWS CloudWatch Logs, removing sensitive information before logging.
B. Before writing to DynamoDB, do a pre-write acknoledgment to disk on the application server, removing sensitive information before logging. Periodically rotate these log files into S3.
C. Use a DynamoDB StreamSpecification and periodically flush to an EC2 instance store, removing sensitive information before putting the objects. Periodically flush these batches to S3.
D. Before writing to DynamoDB, do a pre-write acknoledgment to disk on the application server, removing sensitive information before logging. Periodically pipe these files into CloudWatch Logs.

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

**Explanation/Reference:**
All suggested periodic options are sensitive to server failure during or between periodic flushes. Streaming to Lambda and then logging to CloudWatch Logs will make the system resilient to instance and Availability Zone failures.
Reference: http://docs.aws.amazon.com/lambda/latest/dg/with-ddb.html

**QUESTION 408**
You need your API backed by DynamoDB to stay online during a total regional AWS failure. You can tolerate a couple minutes of lag or slowness during a large failure event, but the system should recover with normal operation after those few minutes.
What is a good approach?

A. Set up DynamoDB cross-region replication in a master-standby configuration, with a single standby in another region. Create an Auto Scaling Group behind an ELB in each of the two regions DynamoDB is running in. Add a Route53Latency DNS Record with DNS Failover, using the ELBs in the two regions as the resource records.
B. Set up a DynamoDB Multi-Region table. Create an Auto Scaling Group behind an ELB in each of the two regions DynamoDB is running in. Add a Route53 Latency DNS Record with DNS Failover, using the ELBs in the two regions as theresource records.
C. Set up a DynamoDB Multi-Region table. Create a cross-region ELB pointing to a cross-region Auto Scaling Group, and direct a Route53 Latency DNS Record with DNS Failover to the crossregion ELB.
D. Set up DynamoDB cross-region replication in a master-standby configuration, with a single standby in another region. Create a cross-region ELB pointing to a cross-region Auto Scaling Group, and direct a Route53 Latency DNS Recordwith DNS Failover to the cross-region ELB.

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

**Explanation/Reference:**
There is no such thing as a cross-region ELB, nor such thing as a cross-region Auto Scaling Group, nor such thing as a DynamoDB Multi-Region Table. The only option that makes sense is the cross-regional replication version with two ELBs and ASGs with Route53 Failover and Latency DNS.
Reference: http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.CrossRegionRepl.html

**QUESTION 409**
You have an asynchronous processing application using an Auto Scaling Group and an SQS Queue. The Auto Scaling Group scales according to the depth of the job queue. The completion velocity of the jobs has gone down, the Auto Scaling Group size has maxed out, but the inbound job velocity did not increase. What is a possible issue?

A. Some of the new jobs coming in are malformed and unprocessable.
B. The routing tables changed and none of the workers can process events anymore.
C. Someone changed the IAM Role Policy on the instances in the worker group and broke permissions to access the queue.
D. The scaling metric is not functioning correctly.



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

**Explanation/Reference:**
The IAM Role must be fine, as if it were broken, NO jobs would be processed since the system would never be able to get any queue messages. The same reasoning applies to the routing table change. The scaling metric is fine, as instance count increased when the queue depth increased due to more messages entering than exiting. Thus, the only reasonable option is that some of the recent messages must be malformed and unprocessable.

**QUESTION 410**
Your company wants to understand where cost is coming from in the company's production AWS account. There are a number of applications and services running at any given time. Without expending too much initial development time, how best can you give the business a good understanding of which applications cost the most per month to operate?

A. Create an automation script which periodically creates AWS Support tickets requesting detailed intra-month information about your bill.
B. Use custom CloudWatch Metrics in your system, and put a metric data point whenever cost is incurred.
C. Use AWS Cost Allocation Tagging for all resources which support it. Use the Cost Explorer to analyze costs throughout the month.
D. Use the AWS Price API and constantly running resource inventory scripts to calculate total price based on multiplication of consumed resources over time.

**Correct Answer:** C

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

**Explanation/Reference:**
Cost Allocation Tagging is a built-in feature of AWS, and when coupled with the Cost Explorer, provides a simple and robust way to track expenses. You can also use tags to filter views in Cost Explorer. Note that before you can filter views by tags in Cost Explorer, you must have applied tags to your resources and activate them, as described in the following sections. For more information about Cost Explorer, see Analyzing Your Costs with Cost Explorer.
Reference:
http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

**QUESTION 411**
There is a very serious outage at AWS. EC2 is not affected, but your EC2 instance deployment scripts stopped working in the region with the outage. What might be the issue?

A. The AWS Console is down, so your CLI commands do not work.
B. S3 is unavailable, so you can't create EBS volumes from a snapshot you use to deploy new volumes.
C. AWS turns off the <code>DeployCode</code> API call when there are major outages, to protect from system floods.
D. None of the other answers make sense. If EC2 is not affected, it must be some other issue.

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



**Explanation/Reference:**
S3 stores all snapshots. If S3 is unavailable, snapshots are unavailable. Amazon EC2 also uses Amazon S3 to store snapshots (backup copies) of the data volumes. You can use snapshots for recovering data quickly and reliably in case of application or system failures. You can also use snapshots as a baseline to create multiple new data volumes, expand the size of an existing data volume, or move data volumes across multiple Availability Zones, thereby making your data usage highly scalable. For more information about using data volumes and snapshots, see Amazon Elastic Block Store.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonS3.html

**QUESTION 412**
Which of the following tools does not directly support AWS OpsWorks, for monitoring your stacks?

A. AWS Config
B. Amazon CloudWatch Metrics
C. AWS CloudTrail
D. Amazon CloudWatch Logs

**Correct Answer:** A

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

**Explanation/Reference:**
You can monitor your stacks in the following ways: AWS OpsWorks uses Amazon CloudWatch to provide thirteen custom metrics with detailed monitoring for each instance in the stack; AWS OpsWorks integrates with AWS CloudTrail to log every AWS OpsWorks API call and store the data in an Amazon S3 bucket; You can use Amazon CloudWatch Logs to monitor your stack's system, application, and custom logs.
Reference: http://docs.aws.amazon.com/opsworks/latest/userguide/monitoring.html

**QUESTION 413**
What is a circular dependency in AWS CloudFormation?

A. When a Template references an earlier version of itself.
B. When Nested Stacks depend on each other.
C. When Resources form a DependOn loop.
D. When a Template references a region, which references the original Template.

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



**Explanation/Reference:**
To resolve a dependency error, add a DependsOn attribute to resources that depend on other resources in your template. In some cases, you must explicitly declare dependencies so that AWS CloudFormation can create or delete resources in the correct order. For example, if you create an Elastic IP and a VPC with an Internet gateway in the same stack, the Elastic IP must depend on the Internet gateway attachment. For additional information, see DependsOn Attribute.
Reference:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html#trouble%20shootin%20g-errors-dependence-error

**QUESTION 414**
You need to run a very large batch data processing job one time per day. The source data exists entirely in S3, and the output of the processing job should also be written to S3 when finished. If you need to version control this processing job and all setup and teardown logic for the system, what approach should you use?

A. Model an AWS EMR job in AWS Elastic Beanstalk.
B. Model an AWS EMR job in AWS CloudFormation.
C. Model an AWS EMR job in AWS OpsWorks.
D. Model an AWS EMR job in AWS CLI Composer.

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

**Explanation**

**Explanation/Reference:**
To declaratively model build and destroy of a cluster, you need to use AWS CloudFormation. OpsWorks and Elastic Beanstalk cannot directly model EMR Clusters. The CLI is not declarative, and CLI Composer does not exist.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-emrcluster.html

**QUESTION 415**
What is true of the way that encryption works with EBS?

A. Snapshotting an encrypted volume makes an encrypted snapshot; restoring an encrypted snapshot creates an encrypted volume when specified / requested.
B. Snapshotting an encrypted volume makes an encrypted snapshot when specified / requested; restoring an encrypted snapshot creates an encrypted volume when specified / requested.
C. Snapshotting an encrypted volume makes an encrypted snapshot; restoring an encrypted snapshot always creates an encrypted volume.
D. Snapshotting an encrypted volume makes an encrypted snapshot when specified / requested; restoring an encrypted snapshot always creates an encrypted volume.

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



**Explanation/Reference:**
Snapshots that are taken from encrypted volumes are automatically encrypted. Volumes that are created from encrypted snapshots are also automatically encrypted. Your encrypted volumes and any associated snapshots always remain protected. For more information, see Amazon EBS Encryption.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

**QUESTION 416**
When thinking of AWS OpsWorks, which of the following is true?

A. Stacks have many layers, layers have many instances.
B. Instances have many stacks, stacks have many layers.
C. Layers have many stacks, stacks have many instances.
D. Layers have many instances, instances have many stacks.

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

**Explanation/Reference:**
The stack is the core AWS OpsWorks component. It is basically a container for AWS resources - Amazon EC2 instances, Amazon RDS database instances, and so on - that have a common purpose and should be logically managed together. You define the stack's constituents by adding one or more layers. A layer represents a set of Amazon EC2 instances that serve a particular purpose, such as serving applications or hosting a database server. An instance represents a single computing resource, such as an Amazon EC2 instance.
Reference: http://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html

**QUESTION 417**
When thinking of AWS Elastic Beanstalk, which statement is true?

A. Worker tiers pull jobs from SNS.
B. Worker tiers pull jobs from HTTP.
C. Worker tiers pull jobs from JSON.
D. Worker tiers pull jobs from SQS.

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

**Explanation/Reference:**
Elastic Beanstalk installs a daemon on each Amazon EC2 instance in the Auto Scaling group to process Amazon SQS messages in the worker environment. The daemon pulls data off the Amazon SQS queue, inserts it into the message body of an HTTP POST request, and sends it to a user-configurable URL path on the local host. The content type for the message body within an HTTP POST request is application/json by default.
Reference:
http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-tiers.html

**QUESTION 418**
Your company needs to automate 3 layers of a large cloud deployment. You want to be able to track this deployment's evolution as it changes over time, and carefully control any alterations. What is a good way to automate a stack to meet these requirements?

A. Use OpsWorks Stacks with three layers to model the layering in your stack.
B. Use CloudFormation Nested Stack Templates, with three child stacks to represent the three logical layers of your cloud.
C. Use AWS Config to declare a configuration set that AWS should roll out to your cloud.
D. Use Elastic Beanstalk Linked Applications, passing the important DNS entires between layers using the metadata interface.

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

**Explanation/Reference:**
Only CloudFormation allows source controlled, declarative templates as the basis for stack automation. Nested Stacks help achieve clean separation of layers while simultaneously providing a method to control all layers at once when needed.

**QUESTION 419**
Your application's Auto Scaling Group scales up too quickly, too much, and stays scaled when traffic decreases.
What should you do to fix this?

A. Set a longer cooldown period on the Group, so the system stops overshooting the target capacity. The issue is that the scaling system does not allow enough time for new instances to begin servicing requests before measuring aggregateload again.
B. Calculate the bottleneck or constraint on the compute layer, then select that as the new metric, and set the metric thresholds to the bounding values that begin to affect response latency.
C. Raise the CloudWatch Alarms threshold associated with your autoscaling group, so the scaling takes more of an increase in demand before beginning.
D. Use larger instances instead of many smaller ones, so the Group stops scaling out so much and wasting resources as the OS level, since the OS uses a higher proportion of resources on smaller instances.

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



**Explanation/Reference:**
Systems will always over-scale unless you choose the metric that runs out first and becomes constrained first. You also need to set the thresholds of the metric based on whether or not latency is affected by the change, to justify adding capacity instead of wasting money.
Reference: http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/policy_creating.html

**QUESTION 420**
You need the absolute highest possible network performance for a cluster computing application. You already selected homogeneous instance types supporting 10 gigabit enhanced networking, made sure that your workload was network bound, and put the instances in a placement group. What is the last optimization you can make?

A. Use 9001 MTU instead of 1500 for Jumbo Frames, to raise packet body to packet overhead ratios.
B. Segregate the instances into different peered VPCs while keeping them all in a placement group, so each one has its own Internet Gateway.
C. Bake an AMI for the instances and relaunch, so the instances are fresh in the placement group and do not have noisy neighbors.
D. Turn off SYN/ACK on your TCP stack or begin using UDP for higher throughput.

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

**Explanation/Reference:**
For instances that are collocated inside a placement group, jumbo frames help to achieve the maximum network throughput possible, and they are recommended in this case. For more information, see Placement Groups.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html#jumbo_frame_instances

**QUESTION 421**
Your CTO is very worried about the security of your AWS account. How best can you prevent hackers from completely hijacking your account?

A. Use short but complex password on the root account and any administrators.
B. Use AWS IAM Geo-Lock and disallow anyone from logging in except for in your city.
C. Use MFA on all users and accounts, especially on the root account.
D. Don't write down or remember the root account password after creating the AWS account.

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

**Explanation/Reference:**
For increased security, we recommend that you configure multi-factor authentication (MFA) to help protect your AWS resources. MFA adds extra security because it requires users to enter a unique authentication code from an approved authentication device or SMS text message when they access AWS websites or services.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

**QUESTION 422**
If you are trying to configure an AWS Elastic Beanstalk worker tier for easy debugging if there are problems finishing queue jobs, what should you configure?

A. Configure Rolling Deployments
B. Configure Enhanced Health Reporting
C. Configure Blue-Green Deployments
D. Configure a Dead Letter Queue

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

**Explanation/Reference:**
Elastic Beanstalk worker environments support Amazon Simple Queue Service (SQS) dead letter queues. A dead letter queue is a queue where other (source) queues can send messages that for some reason could not be successfully processed. A primary benefit of using a dead letter queue is the ability to sideline and

isolate the unsuccessfully processed messages. You can then analyze any messages sent to the dead letter queue to try to determine why they were not successfully processed.

**QUESTION 423**
You have a high security requirement for your AWS accounts.
What is the most rapid and sophisticated setup you can use to react to AWS API calls to your account?

A. Subscription to AWS Config via an SNS Topic. Use a Lambda Function to perform in-flight analysis and reactivity to changes as they occur.
B. Global AWS CloudTrail setup delivering to S3 with an SNS subscription to the deliver notifications, pushing into a Lambda, which inserts records into an ELK stack for analysis.
C. Use a CloudWatch Rule ScheduleExpression to periodically analyze IAM credential logs. Push the deltas for events into an ELK stack and perform ad-hoc analysis there.
D. CloudWatch Events Rules which trigger based on all AWS API calls, submitting all events to an AWS Kinesis Stream for arbitrary downstream analysis.

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

**Explanation/Reference:**



**QUESTION 424**
What method should you use to author automation if you want to wait for a CloudFormation stack to finish completing in a script?

A. Event subscription using SQS.
B. Event subscription using SNS.
C. Poll using <code>ListStacks</code> / <code>list-stacks</code>
D. Poll using <code>GetStackStatus</code> / <code>get-stack-status</code>

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

**Explanation/Reference:**
Event driven systems are good for IFTTT logic, but only polling will make a script wait to complete. ListStacks / list-stacks is a real method, GetStackStatus / get-stack-status is not.
Reference:
http://docs.aws.amazon.com/cli/latest/reference/cloudformation/list-stacks.html

**QUESTION 425**
Your application consists of 10% writes and 90% reads. You currently service all requests through a Route53 Alias Record directed towards an AWS ELB, which sits in front of an EC2 Auto Scaling Group. Your system is getting very expensive when there are large traffic spikes during certain news events, during which many more people request to read similar data all at the same time. What is the simplest and cheapest way to reduce costs and scale with spikes like this?

A. Create an S3 bucket and asynchronously replicate common requests responses into S3 objects. When a request comes in for a precomputed response, redirect to AWS S3.
B. Create another ELB and Auto Scaling Group layer mounted on top of the other system, adding a tier to the system. Serve most read requests out of the top layer.
C. Create a CloudFront Distribution and direct Route53 to the Distribution. Use the ELB as an Origin and specify Cache Behaviours to proxy cache requests which can be served late.
D. Create a Memcached cluster in AWS ElastiCache. Create cache logic to serve requests which can be served late from the in-memory cache for increased performance.

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

**Explanation/Reference:**
CloudFront is ideal for scenarios in which entire requests can be served out of a cache and usage patterns involve heavy reads and spikiness in demand. A cache behavior is the set of rules you configure for a given URL pattern based on file extensions, file names, or any portion of a URL path on your website (e.g., *.jpg). You can configure multiple cache behaviors for your web distribution. Amazon CloudFront will match incoming viewer requests with your list of URL patterns, and if there is a match, the service will honor the cache behavior you configure for that URL pattern. Each cache behavior can include the following Amazon CloudFront configuration values: origin server name, viewer connection protocol, minimum expiration period, query string parameters, cookies, and trusted signers for private content.
Reference: https://aws.amazon.com/cloudfront/dynamic-content/

**QUESTION 426**
You need to perform ad-hoc business analytics queries on well-structured data. Data comes in constantly at a high velocity. Your business intelligence team can understand SQL. What AWS service(s) should you look to first?

A. Kinesis Firehose + RDS
B. Kinesis Firehose + RedShift
C. EMR using Hive
D. EMR running Apache Spark

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

**Explanation/Reference:**
Kinesis Firehose provides a managed service for aggregating streaming data and inserting it into RedShift. RedShift also supports ad-hoc queries over well-structured data using a SQL-compliant wire protocol, so the business team should be able to adopt this system easily.
Reference:
https://aws.amazon.com/kinesis/firehose/details/

**QUESTION 427**
You are building a game high score table in DynamoDB. You will store each user's highest score for each game, with many games, all of which have relatively similar usage levels and numbers of players. You need to be able to look up the highest score for any game.
What is the best DynamoDB key structure?

A. HighestScore as the hash / only key.
B. GameID as the hash key, HighestScore as the range key.
C. GameID as the hash / only key.
D. GameID as the range / only key.

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



**Explanation/Reference:**
Since access and storage for games is uniform, and you need to have ordering within each game for the scores (to access the highest value), your hash (partition) key should be the GameID, and there should be a range key for HighestScore.

**QUESTION 428**
What is server immutability?

A. Not updating a server after creation.
B. The ability to change server counts.
C. Updating a server after creation.
D. The inability to change server counts.

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

**Explanation/Reference:**
... disposable upgrades offer a simpler way to know if your application has unknown dependencies. The underlying EC2 instance usage is considered temporary

or ephemeral in nature for the period of deployment until the current release is active. During the new release, a new set of EC2 instances are rolled out by terminating older instances. This type of upgrade technique is more common in an immutable infrastructure.
Reference:
https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf

**QUESTION 429**
You run a clustered NoSQL database on AWS EC2 using AWS EBS. You need to reduce latency for database response times. Performance is the most important concern, not availability. You did not perform the initial setup, someone without much AWS knowledge did, so you are not sure if they configured everything optimally. Which of the following is NOT likely to be an issue contributing to increased latency?

A. The EC2 instances are not EBS Optimized.
B. The database and requesting system are both in the wrong Availability Zone.
C. The EBS Volumes are not using PIOPS.
D. The database is not running in a placement group.

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

**Explanation/Reference:**
For the highest possible performance, all instances in a clustered database like this one should be in a single Availability Zone in a placement group, using EBS optimized instances, and using PIOPS SSD EBS Volumes. The particular Availability Zone the system is running in should not be important, as long as it is the same as the requesting resources.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

**QUESTION 430**
Fill the blanks: _____ helps us track AWS API calls and transitions, _____ helps to understand what resources we have now, and _____ allows auditing credentials and logins.

A. AWS Config, CloudTrail, IAM Credential Reports
B. CloudTrail, IAM Credential Reports, AWS Config
C. CloudTrail, AWS Config, IAM Credential Reports
D. AWS Config, IAM Credential Reports, CloudTrail

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

**Explanation/Reference:**

You can use AWS CloudTrail to get a history of AWS API calls and related events for your account. This includes calls made by using the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services.
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

**QUESTION 431**
You are creating an application which stores extremely sensitive financial information. All information in the system must be encrypted at rest and in transit. Which of these is a violation of this policy?

A. ELB SSL termination.
B. ELB Using Proxy Protocol v1.
C. CloudFront Viewer Protocol Policy set to HTTPS redirection.
D. Telling S3 to use AES256 on the server-side.

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

**Explanation/Reference:**
Terminating SSL terminates the security of a connection over HTTP, removing the S for "Secure" in HTTPS. This violates the "encryption in transit" requirement in the scenario.
Reference:
http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-listener-config.htm

**QUESTION 432**
You need to scale an RDS deployment. You are operating at 10% writes and 90% reads, based on your logging. How best can you scale this in a simple way?

A. Create a second master RDS instance and peer the RDS groups.
B. Cache all the database responses on the read side with CloudFront.
C. Create read replicas for RDS since the load is mostly reads.
D. Create a Multi-AZ RDS installs and route read traffic to standby.

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

**Explanation/Reference:**
The high-availability feature is not a scaling solution for read-only scenarios; you cannot use a standby replica to serve read traffic. To service read-only traffic, you should use a Read Replica. For more information, see Working with PostgreSQL, MySQL, and MariaDB Read Replicas.

Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

**QUESTION 433**
When thinking of AWS Elastic Beanstalk, the 'Swap Environment URLs' feature most directly aids in what?

A. Immutable Rolling Deployments
B. Mutable Rolling Deployments
C. Canary Deployments
D. Blue-Green Deployments

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

**Explanation/Reference:**
Simply upload the new version of your application and let your deployment service (AWS Elastic Beanstalk, AWS CloudFormation, or AWS OpsWorks) deploy a new version (green). To cut over to the new version, you simply replace the ELB URLs in your DNS records. Elastic Beanstalk has a Swap Environment URLs feature to facilitate a simpler cutover process.
Reference:
https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf



**QUESTION 434**
You need to create a simple, holistic check for your system's general availablity and uptime. Your system presents itself as an HTTP-speaking API. What is the most simple tool on AWS to achieve this with?

A. Route53 Health Checks
B. CloudWatch Health Checks
C. AWS ELB Health Checks
D. EC2 Health Checks

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

**Explanation/Reference:**
You can create a health check that will run into perpetuity using Route53, in one API call, which will ping your service via HTTP every 10 or 30 seconds. Amazon Route 53 must be able to establish a TCP connection with the endpoint within four seconds. In addition, the endpoint must respond with an HTTP status code of 200 or greater and less than 400 within two seconds after connecting.
Reference:

http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-ofendpoints.html

**QUESTION 435**
What is the scope of an EC2 security group?

A. Availability Zone
B. Placement Group
C. Region
D. VPC

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

**Explanation/Reference:**
A security group is tied to a region and can be assigned only to instances in the same region. You can't enable an instance.

**QUESTION 436**
You run accounting software in the AWS cloud. This software needs to be online continuously during the day every day of the week, and has a very static requirement for compute resources. You also have other, unrelated batch jobs that need to run once per day at any time of your choosing. How should you minimize cost?

A. Purchase a Heavy Utilization Reserved Instance to run the accounting software. Turn it off after hours. Run the batch jobs with the same instance class, so the Reserved Instance credits are also applied to the batch jobs.
B. Purchase a Medium Utilization Reserved Instance to run the accounting software. Turn it off after hours. Run the batch jobs with the same instance class, so the Reserved Instance credits are also applied to the batch jobs.
C. Purchase a Light Utilization Reserved Instance to run the accounting software. Turn it off after hours. Run the batch jobs with the same instance class, so the Reserved Instance credits are also applied to the batch jobs.
D. Purchase a Full Utilization Reserved Instance to run the accounting software. Turn it off after hours. Run the batch jobs with the same instance class, so the Reserved Instance credits are also applied to the batch jobs.

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

**Explanation/Reference:**
Because the instance will always be online during the day, in a predictable manner, and there are a sequence of batch jobs to perform at any time, we should run the batch jobs when the account software is off. We can achieve Heavy Utilization by alternating these times, so we should purchase the reservation as such, as this represents the lowest cost. There is no such thing a "Full" level utilization purchases on EC2.

Reference: https://d0.awsstatic.com/whitepapers/Cost_Optimization_with_AWS.pdf

**QUESTION 437**
Which EBS volume type is best for high performance NoSQL cluster deployments?

A. io1
B. gp1
C. standard
D. gp2

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

**Explanation/Reference:**
io1 volumes, or Provisioned IOPS (PIOPS) SSDs, are best for: Critical business applications that require sustained IOPS performance, or more than 10,000 IOPS or 160 MiB/s of throughput per volume, like large database workloads, such as MongoDB.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

**QUESTION 438**
You are building out a layer in a software stack on AWS that needs to be able to scale out to react to increased demand as fast as possible. You are running the code on EC2 instances in an Auto Scaling Group behind an ELB. Which application code deployment method should you use?

A. SSH into new instances that come online, and deploy new code onto the system by pulling it from an S3 bucket, which is populated by code that you refresh from source control on new pushes.
B. Bake an AMI when deploying new versions of code, and use that AMI for the Auto Scaling Launch Configuration.
C. Create a Dockerfile when preparing to deploy a new version to production and publish it to S3. Use UserData in the Auto Scaling Launch configuration to pull down the Dockerfile from S3 and run it when new instances launch.
D. Create a new Auto Scaling Launch Configuration with UserData scripts configured to pull the latest code at all times.

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

**Explanation/Reference:**
The bootstrapping process can be slower if you have a complex application or multiple applications to install. Managing a fleet of applications with several build tools and dependencies can be a challenging task during rollouts. Furthermore, your deployment service should be designed to do faster rollouts to take advantage of Auto Scaling.
Reference:

https://d0.awsstatic.com/whitepapers/overview-of-deployment-options-on-aws.pdf

**QUESTION 439**
You need to perform ad-hoc analysis on log data, including searching quickly for specific error codes and reference numbers. Which should you evaluate first?

A. AWS Elasticsearch Service
B. AWS RedShift
C. AWS EMR
D. AWS DynamoDB

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

**Explanation/Reference:**
Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, operate, and scale Elasticsearch clusters in the AWS cloud. Elasticsearch is a popular opensource search and analytics engine for use cases such as log analytics, real-time application monitoring, and click stream analytics.
Reference:
http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/what-is-amazonelasticsearch-service.html



**QUESTION 440**
Which status represents a failure state in AWS CloudFormation?

A. <code>UPDATE_COMPLETE_CLEANUP_IN_PROGRESS</code>
B. <code>DELETE_COMPLETE_WITH_ARTIFACTS</code>
C. <code>ROLLBACK_IN_PROGRESS</code>
D. <code>ROLLBACK_FAILED</code>

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

**Explanation/Reference:**
ROLLBACK_IN_PROGRESS does not mean CloudFormation failed - it could mean I failed to specify a working solution.
ROLLBACK_FAILED means CloudFormation failed to carry out a valid operation - rolling back changes it attempted to introduce but could not complete.
Reference:
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updatingstacks.html

**QUESTION 441**
What is the scope of an EC2 EIP?

A. Placement Group
B. Availability Zone
C. Region
D. VPC

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

**Explanation/Reference:**
An Elastic IP address is tied to a region and can be associated only with an instance in the same region.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

**QUESTION 442**
For AWS Auto Scaling, what is the first transition state an existing instance enters after leaving steady state in Standby mode?



A. Detaching
B. Terminating:Wait
C. Pending
D. EnteringStandby

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

**Explanation/Reference:**
You can put any instance that is in an InService state into a Standby state. This enables you to remove the instance from service, troubleshoot or make changes to it, and then put it back into service. Instances in a Standby state continue to be managed by the Auto Scaling group. However, they are not an active part of your application until you put them back into service.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AutoScalingGroupLifecycle.html

**QUESTION 443**
You want to pass queue messages that are 1GB each. How should you achieve this?

A. Use Kinesis as a buffer stream for message bodies. Store the checkpoint id for the placement in the Kinesis Stream in SQS.

B. Use the Amazon SQS Extended Client Library for Java and Amazon S3 as a storage mechanism for message bodies.
C. Use SQS's support for message partitioning and multi-part uploads on Amazon S3.
D. Use AWS EFS as a shared pool storage medium. Store filesystem pointers to the files on disk in the SQS message bodies.

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

**Explanation/Reference:**
You can manage Amazon SQS messages with Amazon S3. This is especially useful for storing and retrieving messages with a message size of up to 2 GB. To manage Amazon SQS messages with Amazon S3, use the Amazon SQS Extended Client Library for Java.
Reference:
http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/s3-messages.html

**QUESTION 444**
You are designing a service that aggregates clickstream data in batch and delivers reports to subscribers via email only once per week. Data is extremely spikey, geographically distributed, high-scale, and unpredictable. How should you design this system?

A. Use a large RedShift cluster to perform the analysis, and a fleet of Lambdas to perform record inserts into the RedShift tables. Lambda will scale rapidly enough for the traffic spikes.
B. Use a CloudFront distribution with access log delivery to S3. Clicks should be recorded as querystring GETs to the distribution. Reports are built and sent by periodically running EMR jobs over the access logs in S3.
C. Use API Gateway invoking Lambdas which PutRecords into Kinesis, and EMR running Spark performing GetRecords on Kinesis to scale with spikes. Spark on EMR outputs the analysis to S3, which are sent out via email.
D. Use AWS Elasticsearch service and EC2 Auto Scaling groups. The Autoscaling groups scale based on click throughput and stream into the Elasticsearch domain, which is also scalable. Use Kibana to generate reports periodically.

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

**Explanation/Reference:**
Because you only need to batch analyze, anything using streaming is a waste of money. CloudFront is a Gigabit-Scale HTTP(S) global request distribution service, so it can handle scale, geo-spread, spikes, and unpredictability. The Access Logs will contain the GET data and work just fine for batch analysis and email using EMR. Can you use Amazon CloudFront if you expect usage peaks higher than 10 Gbps or 15,000 RPS? Yes. Complete our request for higher limits here, and we will add more capacity to your account within two business days.
Reference:
https://aws.amazon.com/cloudfront/faqs/

**QUESTION 445**

Your system automatically provisions EIPs to EC2 instances in a VPC on boot. The system provisions the whole VPC and stack at once. You have two of them per VPC. On your new AWS account, your attempt to create a Development environment failed, after successfully creating Staging and Production environments in the same region. What happened?

A. You didn't choose the Development version of the AMI you are using.
B. You didn't set the Development flag to true when deploying EC2 instances.
C. You hit the soft limit of 5 EIPs per region and requested a 6th.
D. You hit the soft limit of 2 VPCs per region and requested a 3rd.

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

**Explanation/Reference:**
There is a soft limit of 5 EIPs per Region for VPC on new accounts. The third environment could not allocate the 6th EIP.
Reference:
http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_vpc

**QUESTION 446**
To monitor API calls against our AWS account by different users and entities, we can use _____ to create a history of calls in bulk for later review, and use _____ for reacting to AWS API calls in real-time.



A. AWS Config; AWS Inspector
B. AWS CloudTrail; AWS Config
C. AWS CloudTrail; CloudWatch Events
D. AWS Config; AWS Lambda

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

**Explanation/Reference:**
CloudTrail is a batch API call collection service, CloudWatch Events enables real-time monitoring of calls through the Rules object interface.
Reference: https://aws.amazon.com/whitepapers/security-at-scale-governance-in-aws/

**QUESTION 447**
How does Amazon RDS multi Availability Zone model work?

A. A second, standby database is deployed and maintained in a different availability zone from master, using synchronous replication.

B. A second, standby database is deployed and maintained in a different availability zone from master using asynchronous replication.
C. A second, standby database is deployed and maintained in a different region from master using asynchronous replication.
D. A second, standby database is deployed and maintained in a different region from master using synchronous replication.

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

**Explanation/Reference:**
In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone.
Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

**QUESTION 448**
Which of these is not an instrinsic function in AWS CloudFormation?

A. Fn::Equals
B. Fn::If
C. Fn::Not
D. Fn::Parse



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

**Explanation/Reference:**
This is the complete list of Intrinsic Functions...: Fn::Base64, Fn::And, Fn::Equals, Fn::If, Fn::Not, Fn::Or, Fn::FindInMap, Fn::GetAtt, Fn::GetAZs, Fn::Join, Fn::Select.
Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-functionreference.html

**QUESTION 449**
Which one of the following is a restriction of AWS EBS Snapshots?

A. Snapshot restorations are restricted to the region in which the snapshots are created.
You cannot share unencrypted snapshots.
B. To share a snapshot with a user in other region the snapshot has to be created in that region first.
C. You cannot share a snapshot containing sensitive data such as an AWS Access Key ID or AWS Secret Access Key.

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

**Explanation**

**Explanation/Reference:**
Shapshots shared with other users are usable in full by the recipient, including but limited to the ability to base modified volumes and snapshots.
Reference:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshotpermissions.html

**QUESTION 450**
What option below is the geographic limit of an EC2 security group?

A. Security groups are global.
B. They are confined to Placement Groups.
C. They are confined to Regions.
D. They are confined to Availability Zones.

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

**Explanation/Reference:**
A security group is tied to a region and can be assigned only to instances in the same region.
You can't enable an instance to communicate with an instance outside its region using security group rules. Traffic from an instance in another region is seen as WAN bandwidth.
Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/resources.html

**QUESTION 451**
If designing a single playbook to run across multiple Linux distributions that have distribution specific commands, what would be the best method to allow a successful run?

A. Enable fact gathering and use the `when' conditional to match the distribution to the task.
B. This is not possible, a separate playbook for each target Linux distribution is required.
C. Use `ignore_errors: true' in the tasks.
D. Use the `shell' module to write your own checks for each command that is ran.

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

**Explanation/Reference:**

Ansible provides a method to only run a task when a condition is met using the `when' declarative. With gather facts enabled, the play has access to the distribution name of the Linux system, thus, tasks can be tailored to a specific distribution and ran only when the condition is met, e.g.: ` - when: ansible_os_family == "Debian"'.
Reference:
http://docs.ansible.com/ansible/playbooks_conditionals.html

**QUESTION 452**
Which is the proper syntax for referencing a variable's value in an Ansible task?

A. ${variable_name}
B. { variable_name }
C. "{{ variable_name }}"
D. @variable_name

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

**Explanation/Reference:**
We use the variable's name to reference the variable which we encapsulate in curly brackets `{{ }}'; however, the YAML syntax dictates that a string beginning with a curly bracket denotes a dictionary value. To get around this, it is proper to wrap the variable declaration in quotes.
Reference:
http://docs.ansible.com/ansible/playbooks_variables.html#hey-wait-a-yaml-gotcha

**QUESTION 453**
If Erin has three clusters of server types that are all managed by Ansible and she needs to provision each cluster so that they are configured with their appropriate NTP server addresses. What is the best method Erin should use in Ansible for managing this?

A. Write a task that scans the network in the target hosts' region for the NTP server, register the resulting address so that the next task can write the NTP configuration.
B. Break down the hosts by region in the Ansible inventory file and assign an inventory group variable the NTP address value for the respective region. The playbook can contain just the single play referencing the NTP variable from theinventory.
C. Create a playbook for each different region and store the NTP address in a variable in the play in the event the NTP server changes.
D. Create three plays, each one has the hosts for their respective regions and set the NTP server address in each task.

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

**Explanation/Reference:**
While all four answers provided are correct, only B is the best choice. Ansible offers the ability to assign variables to groups of hosts in the inventory file. When the playbook is ran it will use the variables assigned to the group, even all the groups are specified in a single playbook run. The respective variables will be available to the play. This is easiest method to run, maintain and write.
Reference:
http://docs.ansible.com/ansible/intro_inventory.html#group-variables

**QUESTION 454**
Which of the following is an invalid variable name in Ansible?

A. host1st_ref
B. host-first-ref
C. Host1stRef
D. host_first_ref

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

**Explanation/Reference:**
Variable names can contain letters, numbers and underscores and should always start with a letter. Invalid variable examples, `host first ref', `1st_host_ref''.
Reference:
http://docs.ansible.com/ansible/playbooks_variables.html#what-makes-a-valid-variable-name

**QUESTION 455**
What are the bare minimum requirements for a valid Ansible playbook?

A. The hosts, connection type, fact gathering, vars and tasks.
B. The hosts declaration and tasks
C. A YAML file with a single line containing `---'.
D. At least one play with at least a hosts declaration

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

**Explanation/Reference:**
Ansible Playbooks are a series of plays and must contain at a minimum, one play. A play generally consists of hosts to run on, a list of tasks, variables and roles, and any additional instructions, such as connection type, fact gathering, remote username, etc. that the tasks will need to complete. The only requirement

for a valid play is to declare the hosts.
Reference:
http://docs.ansible.com/ansible/playbooks_intro.html

**QUESTION 456**
When running a playbook on a remote target host you receive a Python error similar to "[Errno 13] Permission denied: `/home/nick/.ansible/tmp'. What would be the most likely cause of this problem?

A. The user's home or `.ansible' directory on the Ansible system is not writeable by the user running the play.
B. The specified user does not exist on the remote system.
C. The user running `ansible-playbook' must run it from their own home directory.
D. The user's home or `.ansible' directory on the Ansible remote host is not writeable by the user running the play

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

**Explanation/Reference:**
Each task that Ansible runs calls a module. When Ansible uses modules, it copies the module to the remote target system. In the error above it attempted to copy it to the remote user's home directory and found that either the home directory or the `.ansible' directory were not writeable and thus could not continue.
Reference:
http://docs.ansible.com/ansible/modules_intro.html

**QUESTION 457**
When Ansible's connection state is set to `remote', what method of communication does Ansible utilize to run commands on the remote target host?

A. SSH
B. RSH
C. PSExec
D. API call to Ansible client on host

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

**Explanation/Reference:**
Ansible does not require a client/server architecture and makes all remote connections over SSH. Ansible utilizes the Paramiko Python libraries for SSH when the native system OpenSSH libraries do not meet the requirements. Also note, Ansible does require Python be installed on the target host. When the target host is Windows, it uses WinRS

Reference:
http://docs.ansible.com/ansible/intro_getting_started.html#remote-connection-information

**QUESTION 458**
Which resource cannot be defined in an Ansible Playbook?

A. Fact Gathering State
B. Host Groups
C. Inventory File
D. Variables

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

**Explanation/Reference:**
Ansible's inventory can only be specified on the command line, the Ansible configuration file or in environment variables.
Reference:
http://docs.ansible.com/ansible/intro_inventory.html



**QUESTION 459**
When specifying multiple variable names and values for a playbook on the command line, which of the following is the correct syntax?

A. ansible-playbook playbook.yml -e `host="foo" pkg="bar"'
B. ansible-playbook playbook.yml -e `host: "foo", pkg: "bar"'
C. ansible-playbook playbook.yml -e `host="foo"' -e `pkg="bar"'
D. ansible-playbook playbook.yml --extra-vars "host=foo", "pkg=bar"

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

**Explanation/Reference:**
Variables are passed in a single command line parameter, `-e' or `--extra-vars'. They are sent as a single string to the playbook and are space delimited. Because of the space delimeter, variable values must be encapsulated in quotes. Additionally, proper JSON or YAML can be passed, such as: `-e `{"key": "name", "array": ["value1", "value2"]}'.
Reference:
http://docs.ansible.com/ansible/playbooks_variables.html#passing-variables-on-the-commandline

**QUESTION 460**
Ansible provides some methods for controlling how or when a task is ran. Which of the following is a valid method for controlling a task with a loop?

A. - with: <value>
B. - with_items: <value>
C. - only_when: <conditional>
D. - items: <value>

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

**Explanation/Reference:**
Ansible provides two methods for controlling tasks, loops and conditionals. The "with_items" context will allow the task to loop through a list of items, while the `when' context will allow a conditional requirement to be met for the task to run.
Both can be used at the same time.
Reference:
http://docs.ansible.com/ansible/playbooks_conditionals.html#loops-and-conditionals



**QUESTION 461**
Which difference between core modules and extra modules is not correct?

A. Extra modules may one day become core modules
B. Core modules are supported by the Ansible team
C. Core modules are shipped by default with Ansible
D. Extra modules have no support

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

**Explanation/Reference:**
While extra modules are not official modules and thus not supported by the Ansible team, they are indeed supported by their writers and the community.
Reference:
http://docs.ansible.com/ansible/modules_extra.html

**QUESTION 462**
What is the proper (best practice) way to begin a playbook?

A. - hosts: all
B. ...
C. ###
D. ---

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

**Explanation/Reference:**
All YAML files can begin with `---' and end with `...' to indicate where YAML starts and ends. While this is optional, it is considered best practice.
Reference: http://docs.ansible.com/ansible/YAMLSyntax.html

**QUESTION 463**
You have a playbook that includes a task to install a package for a service, put a configuration file for that package on the system and restart the service. The playbook is then run twice in a row. What would you expect Ansible to do on the second run?

A. Remove the old package and config file and reinstall and then restart the service.
B. Take no action on the target host.
C. Check if the package is installed, check if the file matches the source file, if not reinstall it; restart the service.
D. Attempt to reinstall the package, copy the file and restart the service.



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

**Explanation/Reference:**
Ansible follows an idempotence model and will not touch or change the system unless a change is warranted.
Reference:
http://docs.ansible.com/ansible/glossary.html

**QUESTION 464**
Which tool will Ansible not use, even if available, to gather facts?

A. facter
B. lsb_release
C. Ansible setup module
D. ohai

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

**Explanation/Reference:**
Ansible will use its own `setup' module to gather facts for the local system. Additionally, if ohai or facter are installed, those will also be used and all variables will be prefixed with `ohai_' or `facter_' respectively. `lsb_relase' is a Linux tool for determining distribution information.
Reference:
http://docs.ansible.com/ansible/setup_module.html

**QUESTION 465**
If a variable is assigned in the `vars' section of a playbook, where is the proper place to override that variable?

A. Inventory group var
B. playbook host_vars
C. role defaults
D. extra vars



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

**Explanation/Reference:**
In Ansible's variable precedence, the highest precedence is the extra vars option on the command line.
Reference:
http://docs.ansible.com/ansible/playbooks_variables.html#variable-precedence-where-should-iput-a-variable

**QUESTION 466**
If Ansible encounters a resource that does not meet the requirements specified in the play it makes the necessary changes to the resource; however if the resource is already in the desired state Ansible will do nothing. This is an example of which methodology?

A. Idempotency
B. Immutability
C. Convergence
D. Infrastructure as Code

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

**Explanation**

**Explanation/Reference:**
Idempotency states that changes are only made if a resource does not meet the requirement specifications. If a change is made, it is made `in-place' and will not break existing resources.
Reference:
http://docs.ansible.com/ansible/glossary.html

**QUESTION 467**
When writing plays, tasks and playbooks, Ansible fully supports which high level language to describe these?

A. YAML
B. Python
C. XML
D. JSON

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

**Explanation/Reference:**
Section: (none)



This can be bit of a trick question. While Ansible Playbooks in this course are written in YAML, Ansible will accept plays, tasks and playbooks in JSON, as JSON a subset of YAML. However, the preferred and fully supported method is YAML.
Reference: http://docs.ansible.com/ansible/YAMLSyntax.html

**QUESTION 468**
What is the expected behavior if Ansible is called with 'ansible-playbook -i localhost playbook.yml'?

A. Ansible will attempt to read the inventory file named 'localhost'
B. Ansible will run the plays locally.
C. Ansible will run the playbook on the host named 'localhost'
D. Ansible won't run, this is invalid command line syntax

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

**Explanation/Reference:**
Ansible expects an inventory filename with the '-i' option, regardless if it is a valid hostname. For this to execute on the host `localhost' resolves to, a comma needs to be appended to the end.
Reference:
http://docs.ansible.com/ansible/intro_inventory.html#inventory

**QUESTION 469**
The Ansible Inventory system allows many attributes to be defined within it. Which item below is not one of these?

A. Group variables
B. Host groups
C. Include vars
D. Children groups

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

**Explanation/Reference:**
Ansible inventory files cannot reference other files for additional data. If this functionality is needed, it must be done in as a script to create a dynamic inventory.
Reference:
http://docs.ansible.com/ansible/intro_inventory.html

**QUESTION 470**
When writing custom Ansible modules, which language is not supported?

A. Python
B. C++
C. Bash
D. All of the languages listed are supported

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

**Explanation/Reference:**
Ansible modules can be written in any language that is executable on the target system. The only requirement is that the module can write its results as JSON output to STDOUT for Ansible to consume.

Reference:
http://docs.ansible.com/ansible/developing_modules.html

**QUESTION 471**
When specifying more than one conditional requirements for a task, what is the proper method?

A. - when: foo == "hello" and bar == "world"
B. - when: foo == "hello" - when: bar == "world"
C. - when: foo == "hello" && bar == "world"
D. - when: foo is "hello" and bar is "world"

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

**Explanation/Reference:**
Ansible will allow you to stack conditionals using 'and' and 'or'. It requires it to be in the same 'when' statement, comparisons must be '==' for equals or '!=' for not equals and the 'and/or' must be written as such, not '&&/||'.
Reference:
http://docs.ansible.com/ansible/playbooks_conditionals.html#the-when-statement



**QUESTION 472**
Ansible supports running Playbook on the host directly or via SSH. How can Ansible be told to run its playbooks directly on the host?

A. Setting 'connection: local' in the tasks that run locally.
B. Specifying '-type local' on the command line.
C. It does not need to be specified; it is the default.
D. Setting 'connection: local' in the Playbook.

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

**Explanation/Reference:**
Ansible can be told to run locally on the command line with the '-c' option or can be told via the 'connection: local' declaration in the playbook. The default connection method is 'remote'.
Reference:
http://docs.ansible.com/ansible/intro_inventory.html#non-ssh-connection-types

**QUESTION 473**
What is the main difference between calling the commands 'ansible' and 'ansible-playbook' on the command line?

A. 'ansible' is for setting configuration and environment variables which 'ansible-playbook' will use when running plays.
B. 'ansible-playbook' is for running entire Playbooks while 'ansible' is for calling ad-hoc commands.
C. 'ansible-playbook' runs the playbooks by using the 'ansible' command to run the individual plays
D. 'ansible' is for running individual plays and 'ansible-playbook' is for running the entire playbook.

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

**Explanation/Reference:**
The 'ansible' command is for running Ansible ad-hoc commands remotely via SSH. 'ansibleplaybook' is for running Ansible Playbook projects.
Reference:
http://docs.ansible.com/ansible/intro_adhoc.html

**QUESTION 474**
Which answer is the proper syntax for specifying two target hosts on the command line when running an Ansible Playbook?



A. ansible-playbook -h host1.example.com -i all playbook.yml
B. ansible-playbook -i host1.example.com playbook.yml
C. ansible-playbook -h host1.example.com,host2.example.com playbook.yml
D. ansible-playbook -i host1.example.com,host2.example.com playbook.yml

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

**Explanation/Reference:**
Ansible uses the `-i' flag for accepting an inventory file or host. To allow Ansible to determine if you are passing a host list versus an inventory file the list must be comma separated. If a single host is specified, a trailing comma must be present.
Reference:
http://docs.ansible.com/ansible/intro_inventory.html#inventory

**QUESTION 475**
What is the purpose of a Docker swarm worker node?

A. scheduling services

B. service swarm node HTTP API endpoints
C. executing containers
D. maintaining cluster state

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

**Explanation/Reference:**
Manager nodes handle cluster management tasks:
maintaining cluster state scheduling services
serving swarm mode HTTP API endpoints
Worker nodes
Worker nodes are also instances of Docker Engine whose sole purpose is to execute containers. Worker nodes don't participate in the Raft distributed state, make scheduling decisions, or serve the swarm mode HTTP API.
Reference: https://docs.docker.com/engine/swarm/how-swarm-mode-works/nodes/#worker-nodes

**QUESTION 476**
You are building a Docker image with the following Dockerfile. How many layers will the resulting image have?
FROM scratch
CMD /app/hello.sh



A. 2
B. 4
C. 1
D. 3

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

**Explanation/Reference:**
FROM scratch
CMD /app/hello.sh
The image contains all the layers from the base image (only one in this case, since we're building rom scratch), plus a new layer with the CMD instruction, and a read-write container layer.
Reference: https://docs.docker.com/engine/userguide/storagedriver/imagesandcontainers/#sharingpromotes-smaller-images

**QUESTION 477**
What storage driver does Docker generally recommend that you use if it is available?

A. zfs
B. btrfs
C. aufs
D. overlay

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

**Explanation/Reference:**
After you have read the storage driver overview, the next step is to choose the best storage driver for your workloads. In making this decision, there are three high-level factors to consider: If multiple storage drivers are supported in your kernel, Docker has a prioritized list of which storage driver to use if no storage driver is explicitly configured, assuming that the prerequisites for that storage driver are met: If aufs is available, default to it, because it is the oldest storage driver. However, it is not universally available.
Reference:
https://docs.docker.com/engine/userguide/storagedriver/selectadriver/

**QUESTION 478**
In which Docker Swarm model does the swarm manager distribute a specific number of replica tasks among the nodes based upon the scale you set in the desired state?



A. distributed services
B. scaled services
C. replicated services
D. global services

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

**Explanation/Reference:**
A service is the definition of the tasks to execute on the worker nodes. It is the central structure of the swarm system and the primary root of user interaction with the swarm. When you create a service, you specify which container image to use and which commands to execute inside running containers. In the replicated services model, the swarm manager distributes a specific number of replica tasks among the nodes based upon the scale you set in the desired state. For global services, the swarm runs one task for the service on every available node in the cluster. A task carries a Docker container and the commands to run inside the container. It is the atomic scheduling unit of swarm. Manager nodes assign tasks to worker nodes according to the number of replicas set in the service scale. Once a task is assigned to a node, it cannot move to another node. It can only run on the assigned node or fail.
Reference: https://docs.docker.com/engine/swarm/key-concepts/#services-and-tasks

**QUESTION 479**
On which local address does the Docker DNS server listen?

A. 127.0.0.1
B. 127.0.0.111
C. 127.0.0.254
D. 127.0.0.11

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

**Explanation/Reference:**
Note: If you need access to a host's localhost resolver, you must modify your DNS service on the host to listen on a non-localhost address that is reachable from within the container. Note: The DNS server is always at 127.0.0.11.
Reference:
https://docs.docker.com/engine/userguide/networking/configure-dns/



**QUESTION 480**
What are the default memory limit policies for a Docker container?

A. Limited memory, limited kernel memory
B. Unlimited memory, limited kernel memory
C. Limited memory, unlimited kernel memory
D. Unlimited memory, unlimited kernel memory

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

**Explanation/Reference:**
Kernel memory limits are expressed in terms of the overall memory allocated to a container. Consider the following scenarios: Unlimited memory, unlimited kernel memory: This is the default behavior. Unlimited memory, limited kernel memory: This is appropriate when the amount of memory needed by all cgroups is greater than the amount of memory that actually exists on the host machine. You can configure the kernel memory to never go over what is available on the host machine, and containers which need more memory need to wait for it. Limited memory, umlimited kernel memory: The overall memory is limited, but the kernel memory is not. Limited memory, limited kernel memory: Limiting both user and kernel memory can be useful for debugging memory-related problems. If a container is using an unexpected amount of either type of memory, it will run out of memory without affecting other containers or the host machine. Within this setting, if the kernel memory limit is lower than the user memory limit, running out of kernel memory will cause the container to experience an OOM error. If the

kernel memory limit is higher than the user memory limit, the kernel limit will not cause the container to experience an OOM.
Reference:
https://docs.docker.com/engine/admin/resource_constraints/#--kernel-memory-details

**QUESTION 481**
What needs to be done in order to remotely access a Docker daemon running on Linux?

A. add certificate authentication to the docker API
B. change the encryption level to TLS
C. enable the TCP socket
D. bind the Docker API to a unix socket

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

**Explanation/Reference:**
The Docker daemon can listen for Docker Remote API requests via three different types of Socket: unix, tcp, and fd. By default, a unix domain socket (or IPC socket) is created at /var/run/docker.sock, requiring either root permission, or docker group membership. If you need to access the Docker daemon remotely, you need to enable the tcp Socket. Beware that the default setup provides unencrypted and un-authenticated direct access to the Docker daemon - and should be secured either using the built in HTTPS encrypted socket or by putting a secure web proxy in front of it.
Reference:
https://docs.docker.com/engine/reference/commandline/dockerd/#daemon-socket-option

**QUESTION 482**
Which of the following Dockerfile commands cannot be overridden at runtime?

A. VOLUME
B. USER
C. ADD
D. CMD

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

**Explanation/Reference:**
When a developer builds an image from a Dockerfile or when she commits it, the developer can set a number of default parameters that take effect when the image starts up as a container. Four of the Dockerfile commands cannot be overridden at runtime: FROM, MAINTAINER, RUN, and ADD. Everything else has a

corresponding override in docker run. We'll go through what the developer might have set in each Dockerfile instruction and how the operator can override that setting.
Reference:
https://docs.docker.com/engine/reference/run/#overriding-dockerfile-image-defaults

**QUESTION 483**
When deploying to a Docker swarm, which section of the docker-compose file defines configuration related to the deployment and running of services?

A. services
B. build
C. deploy
D. args

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

**Explanation/Reference:**
Specify configuration related to the deployment and running of services. This only takes effect when deploying to a swarm withdocker stack deploy, and is ignored by docker-compose up and docker-compose run.
Reference: https://docs.docker.com/compose/compose-file/#deploy



**QUESTION 484**
You are running a Docker daemon on a Linux host and it becomes unresponsive. Which signal, when sent to a Docker process with the kill command, forces the full stack trace to be logged for debugging purposes?

A. -TRACE
B. -IOTRACE
C. -SIGUSER1
D. -KILLTRACE

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

**Explanation/Reference:**
If the daemon is unresponsive, you can force a full stack trace to be logged by sending a SIGUSR1 signal to the daemon. Linux:
$ sudo kill -SIGUSR1 $(pidof dockerd) Windows Server:
Download docker-signal.

Run the executable with the flag --pid=<PID of daemon>.
Reference:
https://docs.docker.com/engine/admin/#force-a-stack-trace-to-be-logged

**QUESTION 485**
Which of the following is NOT an advantage of Docker's content addressable storage model?

A. random UUIDs improve filesystem performance
B. improved security
C. guarantees data integrity after push, pull, load, and save operations
D. avoids content ID collisions

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

**Explanation/Reference:**
Docker 1.10 introduced a new content addressable storage model. This is a completely new way to address image and layer data on disk. Previously, image and layer data was referenced and stored using a randomly generated UUID. In the new model this is replaced by a secure content hash. The new model improves security, provides a built-in way to avoid ID collisions, and guarantees data integrity after pull, push, load, and save operations. It also enables better sharing of layers by allowing many images to freely share their layers even if they did not come from the same build.
Reference: https://docs.docker.com/engine/userguide/storagedriver/imagesandcontainers/#contentaddressable-storage

**QUESTION 486**
What flag would you use to limit a Docker container's memory usage to 128 megabytes?

A. -memory 128m
B. -m 128m
C. --memory-reservation 128m
D. -m 128MB

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

**Explanation/Reference:**
Docker can enforce hard memory limits, which allow the container to use no more than a given amount of user or system memory, or soft limits, which allow the container to use as much memory as it needs unless certain conditions are met, such as when the kernel detects low memory or contention on the host machine. Some of these options have different effects when used alone or when more than one option is set. Most of these options take a positive integer, followed by a

suffix of b, k, m, g, to indicate bytes, kilobytes, megabytes, or gigabytes.
Option -m or --memory=
Description The maximum amount of memory the container can use. If you set this option, the minimum allowed value is 4m (4 megabyte).
Reference: https://docs.docker.com/engine/admin/resource_constraints/#memory

**QUESTION 487**
What is the only layer in a Docker image that is not read-only?

A. they are all read-only
B. none are read-only
C. the first layer
D. the last layer

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

**Explanation/Reference:**
A Docker image is built up from a series of layers. Each layer represents an instruction in the image's Dockerfile. Each layer except the very last one is read-only.
Reference:
https://docs.docker.com/engine/userguide/storagedriver/imagesandcontainers/#images-andlayers

**QUESTION 488**
When building a Docker image, you are searching through a persistent data volume's logs to provide parameters for the next build. You execute the following command. Which of the operations will cause a failure of the Docker
RUNcommand? RUN cat ./data/log/*.error | grep service_status | grep ERROR

A. the first grep command
B. any one of them
C. the second grep command
D. the cat command

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

**Explanation/Reference:**
Some RUN commands depend on the ability to pipe the output of one command into another, using the pipe character (|), as in the following example:

RUN wget -O - https://some.site | wc -l > /number
Docker executes these commands using the /bin/sh -c interpreter, which only evaluates the exit code of the last operation in the pipe to determine success. In the example above this build step succeeds and produces a new image so long as the wc -lcommand succeeds, even if the wget command fails.
Reference:
https://docs.docker.com/engine/userguide/eng-image/dockerfile_best-practices/#run

**QUESTION 489**
What does the Docker network docker_gwbridge do?

A. allows communication between containers on the same host
B. allows communication between swarm nodes on different hosts
C. allows communication between swarm nodes on the same host
D. allows communication between containers on the different hosts

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

**Explanation/Reference:**
The docker_gwbridge is a local bridge network which is automatically created by Docker in two different circumstances: When you initialize or join a swarm, Docker creates the docker_gwbridge network and uses it for communication among swarm nodes on different hosts. When none of a container's networks can provide external connectivity, Docker connects the container to the docker_gwbridge network in addition to the container's other networks, so that the container can connect to external networks or other swarm nodes.
Reference: https://docs.docker.com/engine/userguide/networking/#the-docker_gwbridge-network

**QUESTION 490**
Which services can be used as optional components of setting up a new Trail in CloudTrail?

A. KMS, SNS and SES
B. CloudWatch, S3 and SNS
C. KMS, Cloudwatch and SNS
D. KMS, S3 and CloudWatch

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

**Explanation/Reference:**
Section: (none)

Key Management Service: The use of AWS KMS is an optional element of CloudTrail, but it allows additional encryption to be added to your Log files when stored on S3 Simple Notification Service: Amazon SNS is also an optional component for CloudTrail, but it allows for you to create notifications, for example when a new log file is delivered to S3 SNS could notify someone or a team via an e-mail. Or it could be used in conjunction with CloudWatch when metric thresholds have been reached. CloudWatch Logs: Again, this is another optional component, but AWS CloudTrail allows you to deliver its logs to AWS Cloudwatch Logs as well as S3 for specific monitoring metrics to take place.
Reference:
https://cloudacademy.com/amazon-web-services/aws-cloudtrail-introduction-course/how-doesaws-cloudtrail-work.html

**QUESTION 491**
What is AWS CloudTrail Processing Library?

A. A static library with CloudTrail log files in a movable format machine code that is directly executable
B. An object library with CloudTrail log files in a movable format machine code that is usually not directly executable
C. A Java library that makes it easy to build an application that reads and processes CloudTrail log files
D. A PHP library that renders various generic containers needed for CloudTrail log files

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



**Explanation/Reference:**
AWS CloudTrail Processing Library is a Java library that makes it easy to build an application that reads and processes CloudTrail log files. You can download CloudTrail Processing Library from GitHub.
Reference:
http://aws.amazon.com/cloudtrail/faqs/

**QUESTION 492**
Using the AWS CLI, which command retrieves CloudTrail trail settings, including the status of the trail itself?

A. aws cloudtrail return-trails
B. aws cloudtrail validate-settings
C. aws cloudtrail get-settings
D. aws cloudtrail describe-trails

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

**Explanation**

**Explanation/Reference:**
Explanation:
You can retrieve trail settings and status using the cloudtrail describe-trails command. It will generate output similar to the example below.


```
{
"trailList": [
{
"IncludeGlobalServiceEvents": false,
"Name": "trailname",
"S3KeyPrefix": "my-prefix",
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
"LogFileValidationEnabled": true,
"IsMultiRegionTrail": true,
"HasCustomEventSelectors": false,
"S3BucketName": " bucket"
"SnsTopicName": " topic",
"HomeRegion": "us-east-2"
}
]
}
```




Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trailby-using-the-aws-cli.htm

**QUESTION 493**
You are running Amazon CloudTrail on an Amazon S3 bucket and look at your most recent log. You notice that the entries include the ListThings and CreateThings actions and wonder if your devices have been hacked. Based on these entries, what service would you be concerned may have been hacked?

A. Amazon Inspector
B. AWS IoT
C. AWS CodePipeline
D. Amazon Glacier

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

**Explanation**

**Explanation/Reference:**
AWS IoT (Internet of Things) is integrated with CloudTrail to capture API calls from the AWS IoT console or from your code to the AWS IoT APIs. AWS IoT provides secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud. Using the information collected by CloudTrail, you can determine the request that was made to AWS IoT, the source IP address from which the request was made, who made the request, when it was made, and so on.
Reference: http://docs.aws.amazon.com/iot/latest/developerguide/monitoring_overview.html#iot-usingcloudtrail

**QUESTION 494**
When logging with Amazon CloudTrail, API call information for services with regional end points is ____.

A. captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket
B. captured, processed, and delivered to the region associated with your Amazon S3 bucket
C. captured in the same region as to which the API call is made and processed and delivered to the region associated with your Amazon S3 bucket
D. captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket

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



**Explanation/Reference:**
When logging with Amazon CloudTrail, API call information for services with regional end points (EC2, RDS etc.) is captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket. API call information for services with single end points (IAM, STS etc.) is captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket.
Reference:
https://aws.amazon.com/cloudtrail/faqs/

**QUESTION 495**
When logging with Amazon CloudTrail, API call information for services with single end points is ____.

A. captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket
B. captured, processed, and delivered to the region associated with your Amazon S3 bucket
C. captured in the same region as to which the API call is made and processed and delivered to the region associated with your Amazon S3 bucket
D. captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket

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

**Explanation/Reference:**
When logging with Amazon CloudTrail, API call information for services with regional end points (EC2, RDS etc.) is captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket. API call information for services with single end points (IAM, STS etc.) is captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket.
Reference:
https://aws.amazon.com/cloudtrail/faqs/

**QUESTION 496**
What is the correct syntax for the AWS command to create a single region trail?

A. aws create-trail --name trailname --s3-object objectname
B. aws cloudtrail --s3-regionname IPaddress create-trail --name trailname
C. aws cloudtrail create-trail --name trailname --s3-bucket-name bucketname
D. aws cloudtrail create-trail --name trailname --s3-portnumber IPaddress



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

**Explanation/Reference:**
The command aws cloudtrail create-trail --name trailname --s3-bucket-name bucketname will create a single region trail. You must create a S3 bucket before you execute the command, with proper CloudTrail permissions applied to it (and you must have the AWS command line tools (CLI) on your system).
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trailby-using-the-aws-cli.html

**QUESTION 497**
You want to set up the CloudTrail Processing Library to log your bucket operations. Which command will build a .jar file from the CloudTrail Processing Library source code?

A. mvn javac mvn -install processor
B. jar install processor
C. build jar -Dgpg.processor
D. mvn clean install -Dgpg.skip=true

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

**Explanation/Reference:**
The CloudTrail Processing Library is a Java library that provides an easy way to process AWS CloudTrail logs in a fault-tolerant, scalable and flexible way. To set up the CloudTrail Processing Library, you first need to download CloudTrail Processing Library source from GitHub. You can then create the .jar file using this command.
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/use-the-cloudtrail-processinglibrary.html

**QUESTION 498**
By default, Amazon CloudTrail logs ____ actions defined by the CloudTrail ____ APIs.

A. bucket-level; RESTful
B. object-level; RESTful
C. object-level; SDK
D. bucket-level; SDK



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

**Explanation/Reference:**
By default, CloudTrail logs bucket-level actions. Amazon S3 records are written together with other AWS service records in a log file. Amazon S3 bucket-level actions supported for logging by CloudTrail are defined in its RESTful API.
Reference: http://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html

**QUESTION 499**
You want to build an application that coordinates work across distributed components, and you find Amazon Simple Workflow Service (Amazon SWF) does this easily. You have enabled logging in CloudTrail, but you are unsure about Amazon SWF actions supported.
Which of the following actions is NOT supported?

A. RegisterDomain
B. RegisterWorkflowActivity
C. RegisterActivityType
D. RegisterWorkflowType

**Correct Answer:** B

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

**Explanation/Reference:**
Amazon SWF is integrated with AWS CloudTrail, a service that captures API calls made by or on behalf of Amazon SWF and delivers the log files to an Amazon S3 bucket that you specify. The API calls can be made indirectly by using the Amazon SWF console or directly by using the Amazon SWF API. When CloudTrail logging is enabled, calls made to Amazon SWF actions are tracked in log files. Amazon SWF records are written together with any other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on a specified time period and file size. The following actions are supported:
DeprecateActivityType
DeprecateDomain
DeprecateWorkflowType
RegisterActivityType
RegisterDomain RegisterWorkflowType
Reference: http://docs.aws.amazon.com/amazonswf/latest/developerguide/ct-logging.html

**QUESTION 500**
Consider the portion of a CloudTrail log file below. Which type of event is being captured?
"eventTime":"2016-07-16T17:35:32Z",
"eventSource":"signin.amazonaws.com",
"eventName":"ConsoleLogin",
"awsRegion":"us-west-1", "sourceIPAddress":"192.1.2.10",
...



A. AWS console sign-in
B. AWS log off
C. AWS error
D. AWS deployment

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

**Explanation/Reference:**
CloudTrail records attempts to sign into the AWS Management Console, the AWS Discussion Forums and the AWS Support Center. Note, however, that CloudTrail does not record root sign-in failures.
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-awsconsole-sign-in-events.html

**QUESTION 501**
Using the AWS CLI, which command would you use to change the configuration settings for a CloudTrail trail?

A. modify-trail
B. change-trail
C. update-trail
D. set-trail

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

**Explanation/Reference:**
The update-trail command is used to change the configuration settings for a trail. You can only run update-trail command from the region in which the trail was created.
Reference:
http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trailby-using-the-aws-cli.html

**QUESTION 502**
As CloudTrail sends a notification each time a log file is written to the Amazon S3 bucket, an account that is very active can generate a large number of notifications. If you subscribe using email or SMS, you may end up receiving a large volume of messages. Which of the following should you use to handle notifications programmatically?



A. Amazon Kinesis Firehose
B. Amazon Simple Queue Service (Amazon SQS)
C. Amazon Simple Email Service (Amazon SES)
D. Amazon AppStream

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

**Explanation/Reference:**
As CloudTrail sends a notification each time a log file is written to the Amazon S3 bucket, an account that's very active can generate a large number of notifications. If you subscribe using email or SMS, you can end up receiving more messages than you can handle. AWS recommends that you subscribe using Amazon Simple Queue Service (Amazon SQS), which lets you handle notifications programmatically.
Reference: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/getting_notifications_configuration.html

**QUESTION 503**
Within an IAM policy, can you add an IfExists condition at the end of a Null condition?

A. Yes, you can add an IfExists condition at the end of a Null condition but not in all Regions.
B. Yes, you can add an IfExists condition at the end of a Null condition depending on the condition.
C. No, you cannot add an IfExists condition at the end of a Null condition.
D. Yes, you can add an IfExists condition at the end of a Null condition.

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

**Explanation/Reference:**
Within an IAM policy, IfExists can be added to the end of any condition operator except the Null condition. It can be used to indicate that conditional comparison needs to happen if the policy key is present in the context of a request; otherwise, it can be ignored.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html

**QUESTION 504**
You are hosting multiple environments in multiple regions and would like to use Amazon Inspector for regular security assessments on your AWS resources across all regions. Which statement about Amazon Inspector's operation across regions is true?

A. Amazon Inspector is a global service that is not region-bound. You can include AWS resources from multiple regions in the same assessment target.
B. Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributedby the service to other Amazon Inspector locations.
C. Amazon Inspector is hosted in each supported region. Telemetry data and findings are shared across regions to provide complete assessment reports.
D. Amazon Inspector is hosted in each supported region separately. You have to create assessment targets using the same name and tags in each region and Amazon Inspector will run against each assessment target in each region.

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

**Explanation/Reference:**
At this time, Amazon Inspector supports assessment services for EC2 instances in only the following AWS regions: US West (Oregon)
US East (N. Virginia)
EU (Ireland)
Asia Pacific (Seoul)
Asia Pacific (Mumbai)
Asia Pacific (Tokyo)
Asia Pacific (Sydney)
Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by the service to other Amazon Inspector locations.

Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_supported_os_regions.html#in%20spector_supported-regions

**QUESTION 505**
To override an allow in an IAM policy, you set the Effect element to _____.

A. Block
B. Stop
C. Deny
D. Allow

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

**Explanation/Reference:**
Section: (none)

By default, access to resources is denied. To allow access to a resource, you must set the Effect element to Allow. To override an allow (for example, to override an allow that is otherwise in force), you set the Effect element to Deny.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

**QUESTION 506**
To access the AWS Security Token Service (STS) you can issue calls directly to the AWS STS Query API. This API is a web service interface that accepts _____ requests.

A. PUT
B. HTTPS
C. POST
D. GET

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

**Explanation/Reference:**
The Query API for IAM and AWS STS lets you call service actions. Query API requests are HTTPS requests that must contain an Action parameter to indicate

the action to be performed. IAM and AWS STS support GET and POST requests for all actions, that is, the API does not require you to use GET for some actions and POST for others.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/programming.html

**QUESTION 507**
A root account has created an IAM group and defined the policy as:

```
"Statement": [
{
"Effect": "Allow"
"Action": ["iam:ChangePassword"],
"Resource": ["arn:aws:iam::123123123123:user/${aws:username}"] },
{
"Effect": "Allow",
"Action": ["iam:GetAccountPasswordPolicy"],
"Resource": ["*"]
}
]
```



What will this policy do?

A. Allow this group to view the password policy of all the users added only to that group
B. Allow all the users of IAM to modify their password
C. Allow an IAM user in this group to view the password policy and modify only his/her password
D. Allow this group to view the password policy of all the IAM users

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

**Explanation/Reference:**
This IAM policy grants access to the ChangePassword action, which lets the users use the console, the CLI, or the API to change their passwords. The Resource element uses a policy variable (aws:username), which is useful in policies that are attached to groups. The aws:username key resolves to the name of the current IAM user when a request is made, so that each user is allowed permission to change only his or her own password . This policy will allow all the users of this group to modify the passwords of all the IAM users.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/HowToPwdIAMUser.html

**QUESTION 508**

For Amazon Inspector's integration with CloudTrail, what information is logged for List* and Describe* APIs?

A. None. Amazon Inspector is an automated service and not monitored by CloudTrail.
B. Both request and response information is logged.
C. Only request information is logged.
D. Request information is always logged. Response information is logged only for Completed assessment runs.

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

**Explanation/Reference:**
For the Amazon Inspector integration with CloudTrail, for the List* and Describe* APIs, only the request information is logged.
Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/logging-using-cloudtrail.html

**QUESTION 509**
A user is defining a policy for the IAM user. Which of the below mentioned elements can be found in an IAM policy?



A. Not Effect
B. Supported Data Types
C. Principal Resource
D. Version Management

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

**Explanation/Reference:**
A user can define various elements for an IAM policy. The elements include Version, ID, Statement, Sid, Effect, Principal, Not Principal, Action, Not Action, Resource, Not Resource, Condition, and Supported Data Types.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

**QUESTION 510**
Which statement is true about configuring proxy support for Amazon Inspector agent on Linuxbased systems?

A. Amazon Inspector proxy support on Linux-based systems is achieved through installing proxyenabled version of the agent which comes with pre-configured files that you need to edit to match your environment.
B. Amazon Inspector agent does NOT support the use of proxy on Linux-based systems.

C. Amazon Inspector proxy configuration on Linux-based system is included in awsagent.env file under /etc/init.d/
D. Amazon Inspector agent proxy settings on Linux-based systems are configured through WinHTTP proxy.

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

**Explanation/Reference:**
To install an AWS agent on an EC2 instance that uses a proxy server Create a file called awsagent.env and save it in the /etc/init.d/ directory. Edit awsagent.env to include these environment variables in the following format:
export https_proxy=https://hostname:port export http_proxy=http://hostname:port export no_proxy= 123.456.789.111 Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents-on-win.html#inspectoragent-proxy

**QUESTION 511**
Some of your EC2 instances are configured to use a Proxy. Can you use Amazon Inspector for regular assessment of instances behind proxy?

A. Only Windows-based systems are supported as Linux-based systems use custom configurations that are not supported by AWS Agent in the current release.
B. Only Linux-based systems are supported, and AWS agent supports HTTPS proxy on these systems.
C. No, AWS Agent does NOT support proxy environments.
D. Yes, AWS Agent supports proxy environments on both Linux-based and Windows-based systems.



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

**Explanation/Reference:**
The AWS agent supports proxy environments. For Linux instances, Inspector supports HTTPS Proxy, and for Windows instances, it supports WinHTTP proxy.
Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents.html

**QUESTION 512**
Amazon Inspector agent collects telemetry data during assessment run and sends this data to Amazon Inspector dedicated S3 bucket for analysis. How can you access telemetry data out of Amazon Inspector and how can you benefit from this data in securing your resources?

A. Telemetry data is kept in S3 and encrypted with a pre-assessment test key configured in KMS, as long as you have access to that key you can download and decrypt telemetry data.
B. Telemetry data is stored in Amazon Inspector dedicated S3 bucket that does NOT belong to your account, Amazon Inspector currently does NOT provide an API or an S3 bucket access mechanism to collected telemetry. Data is retainedtemporarily only to allow for assistance with support requests.
C. Telemetry data is saved on S3 bucket in your account, therefore telemetry data is accessible with proper permissions on that bucket.

D. Telemetry data is deleted immediately after assessment run, therefore data can NOT be accessed or analyzed by any other tools.

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

**Explanation/Reference:**
The telemetry data stored in S3 is retained only to allow for assistance with support requests and is not used or aggregated by Amazon for any other purpose. After 30 days, telemetry data is permanently deleted per a standard Amazon Inspector-dedicated S3 bucket lifecycle policy. At present, Amazon Inspector does not provide an API or an S3 bucket access mechanism to collected telemetry.
Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents.html

**QUESTION 513**
A root owner is trying to create an IAM user of the various departments. The owner has created groups for each department, but wants to still delineate the user based on the sub division level. E.g. The two users from different sub departments should be identified separately and have separate permissions. How can the root owner configure this?

A. Create a hierarchy of the IAM users which are separated based on the department
B. Create a nested group
C. Use the paths to separate the users of the same group
D. It is not possible to delineate within a group



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

**Explanation/Reference:**
The path functionality within an IAM group and user allows them to delineate by further levels. In this case the user needs to use the path with each user or group so that the ARN of the user will look similar to: arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/user1
arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/user2
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_Identifiers.html#Identifiers_ARNs

**QUESTION 514**
A user is defining a policy for an IAM user. Which of the below mentioned options is a valid version defined for the policy?

A. "Version":"2014-01-01"
B. "Version":"2011-10-17"
C. "Version":"2013-10-17"

D. "Version":"2012-10-17"

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

**Explanation/Reference:**
When defining an IAM Policy, the version element specifies the policy language version. Only the following values are allowed:
2012-10-17. This is the current version of the policy language, and the user should use this version number for all the policies.
2008-10-17. This was an earlier version of the policy language. The user might see this version on the existing policies. Do not use this version for any new policies or any existing policies that are being updated. If a version element is not included, the value defaults to 2008-10-17.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html

**QUESTION 515**
Which command will start an assessment run?

A. aws inspector start-assessment-run --assessment-template-arn<template-arn>
B. aws inspector start-assessment-run --assessment-run-name examplerun --assessment-target<target-arn>
C. aws inspector start-assessment-run --assessment-run-name examplerun
D. aws inspector start-assessment-run --assessment-run-name examplerun --assessment-duration<duration-in-seconds>



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

**Explanation/Reference:**
start-assessment-run command requires --assessment-template-arn, other parameters are optional start-assessment-run
--assessment-template-arn <value>
[--assessment-run-name <value>]
[--cli-input-json <value>] [--generate-cli-skeleton <value>]
Reference:
http://docs.aws.amazon.com/cli/latest/reference/inspector/start-assessment-run.html

**QUESTION 516**
Which statement is true about configuring proxy support for Amazon Inspector agent on a Windows-based system?

A. Amazon Inspector agent supports proxy usage on Windows-based systems through the use of the WinHTTP proxy.
B. Amazon Inspector agent supports proxy usage on Linux-based systems but not on Windows.
C. Amazon Inspector proxy support on Windows-based systems is achieved through installing proxy-enabled version of the agent which comes with

preconfigured files that you need to edit to match your environment.

D. Amazon Inspector agent supports proxy usage on Windows-based systems through awsagent.env configuration file.

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

**Explanation/Reference:**
Section: (none)

Proxy support for AWS agents is achieved through the use of the WinHTTP proxy.
Reference:
https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents-on-win.html#inspectoragent-proxy

**QUESTION 517**
What is the default maximum number of Roles per AWS account?



A. 500
B. 250
C. 100
D. There is no limit.

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

**Explanation/Reference:**
The default maximum number of Roles per AWS account is 250.
Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/LimitationsOnEntities.htm

**QUESTION 518**
You have an application which consists of EC2 instances in an Auto Scaling group. Between a particular time frame every day, there is an increase in traffic to your website. Hence users are complaining of a poor response time on the application. You have configured your Auto Scaling group to deploy one new EC2 instance when CPU utilization is greater than 60% for 2 consecutive periods of 5 minutes. What is the least cost-effective way to resolve this problem?

A. Decrease the consecutive number of collection periods
B. Increase the minimum number of instances in the Auto Scaling group

C. Decrease the collection period to ten minutes
D. Decrease the threshold CPU utilization percentage at which to deploy a new instance

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

**Explanation/Reference:**
If you increase the minimum number of instances, then they will be running even though the load is not high on the website. Hence you are incurring cost even though there is no need. All of the remaining options are possible options which can be used to increase the number of instances on a high load. For more information on On-demand scaling, please refer to the below link.
Reference:
http://docs.aws.amazon.com/autoscaling/latest/userguide/as-scale-based-on-demand.html

**QUESTION 519**
You have decided that you need to change the instance type of your production instances which are running as part of an AutoScaling group. The entire architecture is deployed using CloudFormation Template. You currently have 4 instances in Production. You cannot have any interruption in service and need to ensure 2 instances are always runningduring the update. Which of the options below listed can be used for this?



A. AutoScalingRollingUpdate
B. AutoScalingScheduledAction
C. AutoScalingReplacingUpdate
D. AutoScalingIntegrationUpdate

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

**Explanation/Reference:**
Section: (none)

The AWS::AutoScaling::AutoScalingGroup resource supports an UpdatePolicy attribute. This is used to define how an Auto Scalinggroup resource is updated when an update to the Cloud Formation stack occurs. A common approach to updating an Auto Scaling group is to perform a rolling update, which is done by specifying the AutoScalingRollingUpdate policy. This retains the same Auto Scaling group and replaces old instances with new ones, according to the parameters specified. For more information on Autoscaling updates, please refer to the below link.
Reference:
https://aws.amazon.com/premiumsupport/knowledge-center/auto-scaling-group-rolling-updates/

**QUESTION 520**
You currently have the following setup in AWS:
1) An Elastic Load Balancer
2) Auto Scaling Group which launches EC2 Instances
3) AMIs with your code pre-installed You want to deploy the updates of your app to only a certain number of users. You want to have a cost-effective solution. You should also be able to revert back quickly.
Which of the below solutions is the most feasible one?

A. Create a second ELB, and a new Auto Scaling Group assigned a new Launch Configuration. Create a new AMI with the updated app. Use Route53 Weighted Round Robin records to adjust the proportion of traffic hitting the two ELBs.
B. Create new AMIs with the new app. Then use the new EC2 instances in half proportion to the older instances.
C. Redeploy with AWS Elastic Beanstalk and Elastic Beanstalk versions. Use Route 53 Weighted Round Robin records to adjust the proportion of traffic hitting the two ELBs
D. Create a full second stack of instances, cut the DNS over to the new stack of instances, and change the DNS back if a rollback is needed.

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

**Explanation/Reference:**
The Weighted Routing policy of Route53 can be used to direct a proportion of traffic to your application. The best option is to create a second CLB, attach the new Autoscaling Group and then use Route53 to divert the traffic. Option B is wrong because just having EC2 instances running with the new code will not help. Option C is wrong because Clastic beanstalk is good for development environments, and also there is no mention of having 2 environments where environment urls can be swapped. Option D is wrong because you still need Route53 to split the traffic.

**QUESTION 521**
You have an application running a specific process that is critical to the application's functionality, and have added the health check process to your Auto Scaling Group. The instances are showing healthy but the application itself is not working as it should. What could be the issue with the health check, since it is still showing the instances as healthy.

A. You do not have the time range in the health check properly configured
B. It is not possible for a health check to monitor a process that involves the application
C. The health check is not configured properly
D. The health check is not checking the application process

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

**Explanation/Reference:**
If you have custom health checks, you can send the information from your health checks to Auto Scaling so that Auto Scaling can use this information. For example, if you determine that an instance is not functioning as expected, you can set the health status of the instance to Unhealthy. The next time that Auto Scaling performs a health check on the instance, it will determine that the instance is unhealthy and then launch a replacement instance.

**QUESTION 522**
You have just recently deployed an application on EC2 instances behind an ELB. After a couple of weeks, customers are complaining on receiving errors from the application. You want to diagnose the errors and are trying to get errors from the ELB access logs. But the ELB access logs are empty. What is the reason for this.

A. You do not have the appropriate permissions to access the logs
B. You do not have your CloudWatch metrics correctly configured
C. ELB Access logs are only available for a maximum of one week
D. Access logging is an optional feature of Elastic Load Balancing that is disabled by default

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

**Explanation/Reference:**
Clastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Cach log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues. Access logging is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logging for your load balancer. Clastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify. You can disable access logging at any time.

**QUESTION 523**
You have deployed an application to AWS which makes use of Autoscaling to launch new instances. You now want to change the instance type for the new instances. Which of the following is one of the action items to achieve this deployment?

A. Use Elastic Beanstalk to deploy the new application with the new instance type
B. Use Cloudformation to deploy the new application with the new instance type
C. Create a new launch configuration with the new instance type
D. Create new EC2 instances with the new instance type and attach it to the Autoscaling Group

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

**Explanation/Reference:**
The ideal way is to create a new launch configuration, attach it to the existing Auto Scaling group, and terminate the running instances. Option A is invalid because Clastic beanstalk cannot launch new instances on demand. Since the current scenario requires Autoscaling, this is not the ideal option Option B is invalid because this will be a maintenance overhead, since you just have an Autoscaling Group. There is no need to create a whole Cloudformation template for this. Option D is invalid because Autoscaling Group will still launch CC2 instances with the older launch configuration.

**QUESTION 524**
Your application stores sensitive information on an EBS volume attached to your EC2 instance. How can you protect your information? (Choose two.)

A. Unmount the EBS volume, take a snapshot and encrypt the snapshot. Re-mount the Amazon EBS volume.
B. It is not possible to encrypt an EBS volume, you must use a lifecycle policy to transfer data to S3 for encryption.
C. Copy the unencrypted snapshot and check the box to encrypt the new snapshot. Volumes restored from this encrypted snapshot will also be encrypted.
D. Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume. Delete the old Amazon EBS volume.

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

**Explanation/Reference:**
These steps are given in the AWS documentation
To migrate data between encrypted and unencrypted volumes
1) Create your destination volume (encrypted or unencrypted, depending on your need).
2) Attach the destination volume to the instance that hosts the data to migrate.
3) Make the destination volume available by following the procedures in Making an Amazon EBS Volume Available for Use. For Linux instances, you can create a mount point at /mnt/destination and mount the destination volume there.4) Copy the data from your source directory to the destination volume. It may be most convenient to use a bulk-copy utility for this.
To encrypt a volume's data by means of snapshot copying
1) Create a snapshot of your unencrypted CBS volume. This snapshot is also unencrypted.
2) Copy the snapshot while applying encryption parameters. The resulting target snapshot is encrypted.3) Restore the encrypted snapshot to a new volume, which is also encrypted.

**QUESTION 525**
Which Auto Scaling process would be helpful when testing new instances before sending traffic to them, while still keeping them in your Auto Scaling Group?

A. Suspend the process AZ Rebalance
B. Suspend the process Health Check
C. Suspend the process Replace Unhealthy
D. Suspend the process AddToLoadBalancer

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

**Explanation/Reference:**
If you suspend Add To Load Balancer, Auto Scaling launches the instances but does not add them to the load balancer or target group. If you resume the AddTo Load Balancer process. Auto Scaling resumes adding instances to the load balancer or target group when they are launched. However, Auto Scaling does not add the instances that were launched while this process was suspended. You must register those instances manually. Option A is invalid because this just balances the number of CC2 instances in the group across the Availability Zones in the region Option B is invalid because this just checks the health of the instances. Auto Scaling marks an instance as unhealthy if Amazon CC2 or Clastic Load Balancing tells Auto Scaling that the instance is unhealthy. Option C is invalid because this process just terminates instances that are marked as unhealthy and later creates new instances to replace them.

**QUESTION 526**
You have an ELB setup in AWS with EC2 instances running behind it. You have been requested to monitor the incoming connections to the ELB. Which of the below options can suffice this requirement?

A. Use AWSCIoudTrail with your load balancer
B. Enable access logs on the load balancer
C. Use a CloudWatch Logs Agent
D. Create a custom metric CloudWatch filter on your load balancer



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

**Explanation/Reference:**
Clastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Cach log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.
Option A is invalid because this service will monitor all AWS services Option C and D are invalid since CLB already provides a logging feature.

**QUESTION 527**
A DevOps Engineer has been asked to recommend a tool to deploy the components of a threetier web application. This application will use Amazon DynamoDB as a database Which deployment requires the LEAST amount of operational management?

A. Use AWS CloudFormation to create a Classic Load Balancer and an Auto Scaling group. Use AWS OpsWorks to create the application and database resources Deploy application updates with OpsWorks using lifecycle events
B. Use AWS OpsWorks to create a Classic Load Balancer, an Auto Scaling group application, and database resources Deploy application updates using OpsWorks lifecycle events
C. Use AWS OpsWorks to create a Classic Load Balancer Auto Scaling and application resources Use AWS CloudFormation to create the database resources

Deploy application updates using CloudFormation rolling updates

D. Use AWS CloudFormation to create a Classic Load Balancer an Auto Scaling group and database resources Deploy application updates using CloudFormation rolling updates

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

**Explanation/Reference:**

**QUESTION 528**
A company uses AWS CodePipeline to manage and deploy infrastructure as code. The infrastructure is defined in AWS CloudFormation templates and is primarily comprised of multiple Amazon EC2 instances and Amazon RDS databases. The Security team has observed many operators creating inbound security group rules with a source CIDR of 0 0 0 0/0 and would like to proactively stop the deployment of rules with open CIDRs The DevOps Engineer will implement a predeptoyment step that runs some security checks over the CloudFormation template before the pipeline processes it. This check should allow only inbound security group rules with a source CIDR of 0.0.0.0/0 if the rule has the description "Security Approval Ref XXXXX (where XXXXX is a preallocated reference). The pipeline step should fail if this condition is not met and the deployment should be blocked. How should this be accomplished?

A. Enable a SCP in AWS Organizations. The policy should deny access to the API call Create Security GroupRule if the rule specifies 0.0.0.0/0 without a description referencing a security approval.
B. Add an initial stage to CodePipeline called Security Check. This stage should call an AWS Lambda function that scans the CloudFormation template and fails the pipeline if it finds 0.0.0.0/0 in a security group without a descriptionreferencing a security approval.
C. Create an AWS Config rule that is triggered on creation or edit of resource type EC2 SecurityGroup. This rule should call an AWS Lambda function to send a failure notification if the security group has any rules with a source CIDR of
0.0.0.0/0 without a description referencing a security approval.
D. Modify the IAM role used by CodePipeline. The IAM policy should deny access.

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

**Explanation/Reference:**