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

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 during maintenance 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 layer during 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 updates using the credentials in Systems Manager Parameter Store

Correct Answer: A

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 in the 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 auditing account.
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: B

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 that recipe 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 file with 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 the cluster 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: B

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 SNS notifications 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: D

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 a CloudWatch 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 Amazon CloudWatch 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 rule to trigger a daily Lambda function that terminates all instances with this tag.

Correct Answer: A

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.

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: D

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 Events rule 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 cost center, 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: D

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 name the 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 those parameters 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 a maximum 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 the missing 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: C

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 instances have 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 Inspector API 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 EC2 instance 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-place security assessment for each AMI.

Correct Answer: A

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: C

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 and deploy 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 AWS CodeDeploy 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 AWS CodeDeploy 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 a blue/green deployment.

Correct Answer: A

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

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. Implement Amazon 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 Load Balancer 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 DynamoDB Auto Scaling. Use Amazon Route 53 to point the application DNS record to the Elastic Beanstalk load balancer.

Correct Answer: B

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: ORjJns3At2mlh4O4tm0+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@10.25.15.23 :/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

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 Lambda function 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. Change the 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 IP addresses. 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 so that 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

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": [
    "CodePipline 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: A

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: C

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-region replication 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. In the 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, copy the 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 second region 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: B

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

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

Explanation/Reference:
Reference: https://yabhinav.github.io/cloud/awslambda-slack-notifications/

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. Create an 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 to perform 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 the failover 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

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 use Amazon 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 the S3 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 from config 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 Amazon SNS when new data is written to the S3 bucket.

Correct Answer: C

QUESTION 26

A DevOps Engineer has a single Amazon DynamoDB table that received 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 DynamoDB 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: B

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

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

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: C

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

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 the deployment happens with zero downtime.

Correct Answer: CD

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. Store the 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 Lambda function. 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 AMI identification output in an Amazon DynamoDB table.

Correct Answer: B

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 are updated 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 the Application 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 deployed environment 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 Auto Scaling group.

Correct Answer: B

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 and interval.
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 shift percentage 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 select the 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 Lambda function to deploy the code over time at the required percentage.

Correct Answer: C

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 instances launched 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: B

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 Route 53 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 a latency 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 recovery region'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 record set with a failover routing policy.

Correct Answer: D

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: D

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 with the same properties as the instance to be upgraded. Perform a second `Update Stack` operation.
C. Update the `DBEngineVersion` property of the `AWS::RDS::DBInstance` 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 to be 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: B

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_by` details. 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 the `initiated_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: C

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 Amazon DynamoDB 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 up another 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 of noncompliant 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

QUESTION 41
According to Information Security Policy, changes to the contents of objects inside production Amazon S3 bucket 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: D

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

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

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 a separate 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: C

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

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 reduce the 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 to search 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 Amazon Elasticsearch 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 an AWS 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

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 specified subset of customers and monitoring 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 AWS Lambda 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: Canary10Percent15Minutes`.

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

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 CI/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: A

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 service token. 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 the newly 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

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: AB

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: ADE

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 the deployment 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 previously deployed 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

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

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 securely

How 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 environment the 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 the tags 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 all environments.
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 function that 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

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 script to 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 called logs, 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 Run Command script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

Correct Answer: D

QUESTION 56
A publishing company used 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. 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 Varnish 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

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, acquire an 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. Create an 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 data script 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 the DynamoDB table. Monitor each instance and, in case of failure, replace the instance, then manually update the DynamoDB table.

Correct Answer: B

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 `WebsiteConfiguration` 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: D

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 build artifacts 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-stage build-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. After a 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 in another region and passes the build artifact location. The pipeline uses the artifact location and deploys applications in the new region.

Correct Answer: B

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 the DNS 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 new version. 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 is considered stable, promote it to a production release

Correct Answer: AE

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. 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 input from 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 custom action that runs on hardware hosted on premises. The job worker handles running security checks with the on-premises code analysis tool and then returns the job results to CodePipeline. Have the pipeline 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, the web 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 a custom script action after the source stage.

Correct Answer: B

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 this information 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 as part 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 this information 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 lifecycle hook in the appspec.yml file.

Correct Answer: B

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 provides permission 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 this Docker 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 custom recipe 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 configure the 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: B

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, use Amazon 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 the AWS_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 the AWS_RISK_CREDENTIALS_EXPOSED event, set the target of the CloudWatch Events rule to Step Functions.

Correct Answer: A

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 the Lambda 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 the AWS 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 an 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: B

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 post the 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

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 Lambda functions 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 to retrieve 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 each CodePipeline 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 Lambda function code to an Amazon S3 bucket. Set up the deployment step to deploy the Lambda functions from the S3 bucket.

Correct Answer: C

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 a deploy 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 uses Amazon 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 the team and add a deploy action to deploy the application to the next stage.

Correct Answer: B

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 S3 SSE-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-Managed Keys (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 KMS encryption 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

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 appsec.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 appsec.yml to delete the temporary files.

Correct Answer: B

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 business hours 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 minimum number 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 of instances. 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 the close of business.

Correct Answer: B

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 the Finance team.

Correct Answer: B

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 second AZ, 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 when the first instance fails. Use a single-node Aurora instance.

Correct Answer: C

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 to production.
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 review the 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 to an 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

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 IAM role 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 decrypt only 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 allows decryption 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 role associated to the instance profile for CodeDeploy-managed instances and the role used for on-premises instances registration on CodeDeploy.

Correct Answer: C

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 merge code 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

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: B

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 Puppet master. 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 the Auto 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 the Puppet 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 Puppet master. 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: C
Section: (none)

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 the application 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 to disable 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 Lambda function 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 by AWS Config, and then disable the access key so it cannot be used.

Correct Answer: B

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. This Lambda 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 flow logs 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: B

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 Elastic Beanstalk 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 to search 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 Elastic Beanstalk 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 Data Firehouse into Amazon ES. Delete and create a new Amazon ES domain every 90 days.

Correct Answer: A

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

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

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 load balancer 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 the Amazon 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 to accept 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 and only 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: C

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 the Elasticsearch 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 Amazon ES for analysis. Use the Elasticsearch API for querying the data.

Correct Answer: D

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 a lifecycle 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 Lambda function 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 a snapshot 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 the master. 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

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 Config rules 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 encrypted data and notify via Amazon 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 and configure 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 periodically check for non-encrypted S3 objects and EBS volumes, and to ensure that RDS storage is encrypted.

Correct Answer: D

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

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: D

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 Application team 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 Application team 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 the pipeline 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 the Application team changes the application code.

Correct Answer: C

QUESTION 91
The Deployment 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, and there have been service limit alerts for the count of Amazon S3 buckets.
Which pipeline option will reduce S3 bucket sprawl alerts?

A. Combine the multiple separate code repositories into a single one, and deploy using a global 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 global 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 for 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

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 and flexible 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 for the 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 property file 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 Manager Parameter 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

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 in-place 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

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 two environments. 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 Elastic Beanstalk 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 environment as workloads are successfully validated. Keep the old production environment in place until the new staging environment handles all traffic.

Correct Answer: D

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 State Change 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 delete compromised 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 the Security 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

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: BD

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 all findings to Amazon Kinesis Data Firehouse, 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 and 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 Firehouse, 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 account to send all findings to Amazon Kinesis Data Streams. Write and application using KCL to read data from Kinesis Data Streams and write to the S3 bucket.

Correct Answer: D

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 deployment issues.

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: C

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 elect the Amazon RDS master in the disaster recovery region.
B. Create a new Application Load Balancer and Auto Scaling group in the disaster recovery region.
C. Extend the current 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 elect the RDS master.

Correct Answer: BDE

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 on EC2 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 on EC2 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 Run Command 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 Run Command on Amazon EC2 for uploading backup logs to Amazon S3. Use Amazon SES to notify admins with backup activity metadata.

Correct Answer: A

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: B

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 restraining the web server process when memory is full, and deploy it with AWS Systems Manager.

Correct Answer: A

QUESTION 103
A DevOps Engineer is launching a new application that will be deployed 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 sudden 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 read and write capacities.

Correct Answer: CD

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

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

Correct Answer: C

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, and if 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 security headers.
D. set 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 the whitelist.

Correct Answer: C

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 contains the 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 the auto-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 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 the application 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

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 that merges the hotfix tag into the master branch.

B. Create a hotfix branch from the master branch. Triger 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. Triger 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 CodeBuild to run unit tests. Add a manual approval stage that merges the hotfix branch into the master branch.

Correct Answer: B

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 AWS Lambda-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 the instance.
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 Lambda function to create the AMI.

Correct Answer: D

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 EC2 instance.
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 an IPv6 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 the default 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 create a rule in the security group that allows inbound traffic from anywhere.

Correct Answer: D

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 dissociate the Elastic IP address from the instance, and alert the Security team.
B. Attach an IAM policy to the Developer's 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 the Security 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 as production, 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 Security team if an instance has an Elastic IP address associated with it.

Correct Answer: B

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 process and upload it to the new Lightsail test server using the AWS CLI. Test the application, 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 build and 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 for production. 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 instance layer. 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

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

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: B

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? (Select 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: ACE

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 place them in an Amazon S3 bucket for analysis.

Correct Answer: C

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 the integration 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

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

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

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

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

Explanation/Reference:
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html

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:
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.

Every change must go through unit testing.
Every change must go through a suite of functional testing to ensure functionality.
In addition, the company has the following requirements for automation:
Code changes should automatically trigger the CI/CD pipellline.
Any failure in the pipeline should notify devops-admin@xyz.com.
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 CloudWatch metrics 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 pipeline stages 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 CloudWatch Events 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 in pipeline stages and Amazon SES for emailing devops-admin@xyz.com.

Correct Answer: A

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: A

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 and complete 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 webhook URL.
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 the event 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. Parametrize the URL so each pipeline can send to a different URL based on the pipeline environment.

Correct Answer: C

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 IAM group 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 the products 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 constrained templates and CloudFormation. Create a separate group for experts giving them access to the unconstrained templates, CloudFormation, and other AWS services.

Correct Answer: C

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 needed to 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 with the 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

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.HalfAtAtime configuration 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 with additional 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 deployment configuration 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 a deployment strategy with a batch size of 50%.

Correct Answer: C

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 ECS cluster. 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 container image 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 the `create-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 by changes 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

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 Firehouse, and select Amazon ES as the destination for providing storage and search capability.

Correct Answer: C

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: D

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 90 days. 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 an AWS 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 and aggregated. 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 the event 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

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 API Gateway 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 the CloudFront distribution.

Correct Answer: B

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 Systems Operator 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 53 to 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 to the secondary region when a primary database fails.

Correct Answer: B

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

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:CDE

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: C

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: C

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

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

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: B

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: C