formatted_questions_final_cleaned

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

QUESTION 1
A company has a mobile application that makes HTTP API calls to an Application Load Balancer (ALB). The ALB routes requests to an AWS Lambda function. Many different versions of the application are in use at any given time, including versions that are in testing by a subset of users. The version of the application is defined in the user-agent header that is sent with all requests to the API.After a series of recent changes to the API, the company has observed issues with the application. The company needs to gather a metric for each API operation by response code for each version of the application that is in use. A DevOps engineer has modified the Lambda function to extract the API operation name, version information from the user-agent header and response code.Which additional set of actions should the DevOps engineer take to gather the required metrics?

A. Modify the Lambda function to write the API operation name, response code, and version number as a log line to an Amazon CloudWatch Logs log group. Configure a CloudWatch Logs metric filter that increments a metric for each API operation name. Specify response code and application version as dimensions for the metric.
B. Modify the Lambda function to write the API operation name, response code, and version number as a log line to an Amazon CloudWatch Logs log group. Configure a CloudWatch Logs Insights query to populate CloudWatch metrics from the log lines. Specify response code and application version as dimensions for the metric.
C. Configure the ALB access logs to write to an Amazon CloudWatch Logs log group. Modify the Lambda function to respond to the ALB with the API operation name, response code, and version number as response metadata. Configure a CloudWatch Logs metric filter that increments a metric for each API operation name. Specify response code and application version as dimensions for the metric.
D. Configure AWS X-Ray integration on the Lambda function. Modify the Lambda function to create an X-Ray subsegment with the API operation name, response code, and version number. Configure X-Ray insights to extract an aggregated metric for each API operation name and to publish the metric to Amazon CloudWatch. Specify response code and application version as dimensions for the metric.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A security review has identified that an AWS CodeBuild project is downloading a database population script from an Amazon S3 bucket using an unauthenticated request. The security team does not allow unauthenticated requests to S3 buckets for this project.How can this issue be corrected in the MOST secure manner?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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 DevOps engineer manages the Kinesis consumer application, which also runs on Amazon EC2.Sudden increases of data cause the Kinesis consumer application to fall behind, and the Kinesis data streams drop records before the records can be processed. The DevOps engineer must implement a solution to improve stream handling.Which solution meets these requirements with the MOST operational efficiency?

A. Modify the Kinesis consumer application to store the logs durably in Amazon S3. Use Amazon EMR to process the data directly on Amazon S3 to derive customer insights. Store the results in Amazon S3.
B. Horizontally scale the Kinesis consumer application by adding more EC2 instances based on the Amazon CloudWatch GetRecords.IteratorAgeMilliseconds metric. Increase the retention period of the Kinesis data streams.
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 application processes the data faster.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A company recently created a new AWS Control Tower landing zone in a new organization in AWS Organizations. The landing zone must be able to demonstrate compliance with the Center for Internet Security (CIS) Benchmarks for AWS Foundations.The companyâ€™s security team wants to use AWS Security Hub to view compliance across all accounts. Only the security team can be allowed to view aggregated Security Hub findings. In addition, specific users must be able to view findings from their own accounts within the organization. All accounts must be enrolled in Security Hub after the accounts are created.Which combination of steps will meet these requirements in the MOST automated way? (Choose three.)

A. Turn on trusted access for Security Hub in the organizationâ€™s management account. Create a new security account by using AWS Control Tower. Configure the new security account as the delegated administrator account for Security Hub. In the new security account, provide Security Hub with the CIS Benchmarks for AWS Foundations standards.
B. Turn on trusted access for Security Hub in the organizationâ€™s management account. From the management account, provide Security Hub with the CIS Benchmarks for AWS Foundations standards.
C. Create an AWS IAM Identity Center (AWS Single Sign-On) permission set that includes the required permissions. Use the CreateAccountAssignment API operation to associate the security team users with the permission set and with the delegated security account.
D. Create an SCP that explicitly denies any user who is not on the security team from accessing Security Hub.
E. In Security Hub, turn on automatic enablement.
F. In the organizationâ€™s management account, create an Amazon EventBridge rule that reacts to the CreateManagedAccount event. Create an AWS Lambda function that uses the Security Hub CreateMembers API operation to add new accounts to Security Hub. Configure the EventBridge rule to invoke the Lambda function.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A company runs applications in AWS accounts that are in an organization in AWS Organizations. The applications use Amazon EC2 instances and Amazon S3.The company wants to detect potentially compromised EC2 instances, suspicious network activity, and unusual API activity in its existing AWS accounts and in any AWS accounts that the company creates in the future. When the company detects one of these events, the company wants to use an existing Amazon Simple Notification Service (Amazon SNS) topic to send a notification to its operational support team for investigation and remediation.Which solution will meet these requirements in accordance with AWS best practices?

A. In the organization's management account, configure an AWS account as the Amazon GuardDuty administrator account. In the GuardDuty administrator account, add the companyâ€™s existing AWS accounts to GuardDuty as members. In the GuardDuty administrator account, create an Amazon EventBridge rule with an event pattern to match GuardDuty events and to forward matching events to the SNS topic.
B. In the organizationâ€™s management account, configure Amazon GuardDuty to add newly created AWS accounts by invitation and to send invitations to the existing AWS accounts. Create an AWS CloudFormation stack set that accepts the GuardDuty invitation and creates an Amazon EventBridge rule. Configure the rule with an event pattern to match GuardDuty events and to forward matching events to the SNS topic. Configure the CloudFormation stack set to deploy into all AWS accounts in the organization.
C. In the organizationâ€™s management account, create an AWS CloudTrail organization trail. Activate the organization trail in all AWS accounts in the organization. Create an SCP that enables VPC Flow Logs in each account in the organization. Configure AWS Security Hub for the organization. Create an Amazon EventBridge rule with an event pattern to match Security Hub events and to forward matching events to the SNS topic.
D. In the organizationâ€™s management account, configure an AWS account as the AWS CloudTrail administrator account. In the CloudTrail administrator account, create a CloudTrail organization trail. Add the companyâ€™s existing AWS accounts to the organization trail. Create an SCP that enables VPC Flow Logs in each account in the organization. Configure AWS Security Hub for the organization. Create an Amazon EventBridge rule with an event pattern to match Security Hub events and to forward matching events to the SNS topic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A company's DevOps engineer is working in a multi-account environment. The company uses AWS Transit Gateway to route all outbound traffic through a network operations account. In the network operations account, all account traffic passes through a firewall appliance for inspection before the traffic goes to an internet gateway.The firewall appliance sends logs to Amazon CloudWatch Logs and includes event severities of CRITICAL, HIGH, MEDIUM, LOW, and INFO. The security team wants to receive an alert if any CRITICAL events occur.What should the DevOps engineer do to meet these requirements?

A. Create an Amazon CloudWatch Synthetics canary to monitor the firewall state. If the firewall reaches a CRITICAL state or logs a CRITICAL event, use a CloudWatch alarm to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email address to the topic.
B. Create an Amazon CloudWatch metric filter by using a search for CRITICAL events. Publish a custom metric for the finding. Use a CloudWatch alarm based on the custom metric to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email address to the topic.
C. Enable Amazon GuardDuty in the network operations account. Configure GuardDuty to monitor flow logs. Create an Amazon EventBridge event rule that is invoked by GuardDuty events that are CRITICA

D. Use AWS Firewall Manager to apply consistent policies across all accounts. Create an Amazon EventBridge event rule that is invoked by Firewall Manager events that are CRITICA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A company is divided into teams. Each team has an AWS account, and all the accounts are in an organization in AWS Organizations. Each team must retain full administrative rights to its AWS account. Each team also must be allowed to access only AWS services that the company approves for use. AWS services must gain approval through a request and approval process.How should a DevOps engineer configure the accounts to meet these requirements?

A. Use AWS CloudFormation StackSets to provision IAM policies in each account to deny access to restricted AWS services. In each account, configure AWS Config rules that ensure that the policies are attached to IAM principals in the account.
B. Use AWS Control Tower to provision the accounts into OUs within the organization. Configure AWS Control Tower to enable AWS IAM Identity Center (AWS Single Sign-On). Configure IAM Identity Center to provide administrative access. Include deny policies on user roles for restricted AWS services.
C. Place all the accounts under a new top-level OU within the organization. Create an SCP that denies access to restricted AWS services. Attach the SCP to the OU.
D. Create an SCP that allows access to only approved AWS services. Attach the SCP to the root OU of the organization. Remove the FullAWSAccess SCP from the root OU of the organization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A DevOps engineer used an AWS CloudFormation custom resource to set up AD Connector. The AWS Lambda function ran and created AD Connector, but CloudFormation is not transitioning from CREATE_IN_PROGRESS to CREATE_COMPLETE.Which action should the engineer take to resolve this issue?

A. Ensure the Lambda function code has exited successfully.
B. Ensure the Lambda function code returns a response to the pre-signed URL.
C. Ensure the Lambda function IAM role has cloudformation:UpdateStack permissions for the stack ARN.
D. Ensure the Lambda function IAM role has ds:ConnectDirectory permissions for the AWS account.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A company 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 main branch when the changes are ready for production.The developers should not be able to push changes directly to the main branch. The company

applied the AWSCodeCommitPowerUser managed policy to the developersâ€™ IAM role, and now these developers can push changes to the main branch directly on every repository in the AWS account.What should the company do to restrict the developersâ€™ ability to push changes to the main branch directly?

A. Create an additional policy to include a Deny rule for the GitPush and PutFile actions. Include a restriction for the specific repositories in the policy statement with a condition that references the main branch.
B. Remove the IAM policy, and add an AWSCodeCommitReadOnly managed policy. Add an Allow rule for the GitPush and PutFile actions for the specific repositories in the policy statement with a condition that references the main branch.
C. Modify the IAM policy. Include a Deny rule for the GitPush and PutFile actions for the specific repositories in the policy statement with a condition that references the main branch.
D. Create an additional policy to include an Allow rule for the GitPush and PutFile actions. Include a restriction for the specific repositories in the policy statement with a condition that references the feature branches.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A company manages a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances run in an Auto Scaling group across multiple Availability Zones. The application uses an Amazon RDS for MySQL DB instance to store the data. The company has configured Amazon Route 53 with an alias record that points to the ALB.A new company guideline requires a geographically isolated disaster recovery (DR) site with an RTO of 4 hours and an RPO of 15 minutes.Which DR strategy will meet these requirements with the LEAST change to the application stack?

A. Launch a replica environment of everything except Amazon RDS in a different Availability Zone. Create an RDS read replica in the new Availability Zone, and configure the new stack to point to the local RDS DB instance. Add the new stack to the Route 53 record set by using a health check to configure a failover routing policy.
B. Launch a replica environment of everything except Amazon RDS in a different AWS Region. Create an RDS read replica in the new Region, and configure the new stack to point to the local RDS DB instance. Add the new stack to the Route 53 record set by using a health check to configure a latency routing policy.
C. Launch a replica environment of everything except Amazon RDS in a different AWS Region. In the event of an outage, copy and restore the latest RDS snapshot from the primary Region to the DR Region. Adjust the Route 53 record set to point to the ALB in the DR Region.
D. Launch a replica environment of everything except Amazon RDS in a different AWS Region. Create an RDS read replica in the new Region, and configure the new environment to point to the local RDS DB instance. Add the new stack to the Route 53 record set by using a health check to configure a failover routing policy. In the event of an outage, promote the read replica to primary.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 for Oracle DB instance and Amazon DynamoDB. There are separate environments for development, testing, and production.What is the MOST secure and flexible way to obtain password credentials during deployment?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
The security team depends on AWS CloudTrail to detect sensitive security issues in the companyâ€™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 EventBridge 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 EventBridge rule.
B. Deploy the AWS-managed CloudTrail-enabled AWS Config rule, set with a periodic interval of 1 hour. Create an Amazon EventBridge 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 EventBridge rule.
C. Create an Amazon EventBridge rule for a scheduled event every 5 minutes. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on a CloudTrail trail in the AWS account. Add the Lambda function ARN as a target to the EventBridge rule.
D. Launch a t2.nano instance with a script running every 5 minutes that uses the AWS SDK to query CloudTrail in the current account. If the CloudTrail trail is disabled, have the script re-enable the trail.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
An ecommerce company has chosen AWS to host its new platform. The company's DevOps team has started building an AWS Control Tower landing zone. The DevOps team has set the identity store within AWS IAM Identity Center (AWS Single Sign-On) to external identity provider (IdP) and has configured SAML 2.0.The DevOps team wants a robust permission model that applies the principle of least privilege. The model must allow the team to build and manage only the team's own resources.Which combination of steps will meet these requirements? (Choose three.)

A. Create IAM policies that include the required permissions. Include the aws:PrincipalTag condition key.
B. Create permission sets. Attach an inline policy that includes the required permissions and uses the aws:PrincipalTag condition key to scope the permissions.
C. Create a group in the Id
D. Create a group in the Id
E. Enable attributes for access control in IAM Identity Center. Apply tags to users. Map the tags as key-value

pairs.

F. Enable attributes for access control in IAM Identity Center. Map attributes from the IdP as key-value pairs.

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A company uses AWS CodeArtifact to centrally store Python packages. The CodeArtifact repository is configured with the following repository policy:A development team is building a new project in an account that is in an organization in AWS Organizations. The development team wants to use a Python library that has already been stored in the CodeArtifact repository in the organization. The development team uses AWS CodePipeline and AWS CodeBuild to build the new application. The CodeBuild job that the development team uses to build the application is configured to run in a VPC. Because of compliance requirements, the VPC has no internet connectivity.The development team creates the VPC endpoints for CodeArtifact and updates the CodeBuild buildspec.yaml file. However, the development team cannot download the Python library from the repository.Which combination of steps should a DevOps engineer take so that the development team can use CodeArtifact? (Choose two.)

A. Create an Amazon S3 gateway endpoint. Update the route tables for the subnets that are running the CodeBuild job.
B. Update the repository policyâ€™s Principal statement to include the ARN of the role that the CodeBuild project uses.
C. Share the CodeArtifact repository with the organization by using AWS Resource Access Manager (AWS RAM).
D. Update the role that the CodeBuild project uses so that the role has sufficient permissions to use the CodeArtifact repository.
E. Specify the account that hosts the repository as the delegated administrator for CodeArtifact in the organization.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A company uses a series of individual Amazon CloudFormation templates to deploy its multi-Region applications. These templates must be deployed in a specific order. The company is making more changes to the templates than previously expected and wants to deploy new templates more efficiently. Additionally, the data engineering team must be notified of all changes to the templates.What should the company do to accomplish these goals?

A. Create an AWS Lambda function to deploy the CloudFormation templates in the required order. Use stack policies to alert the data engineering team.
B. Host the CloudFormation templates in Amazon S3. Use Amazon S3 events to directly trigger CloudFormation updates and Amazon SNS notifications.
C. Implement CloudFormation StackSets and use drift detection to trigger update alerts to the data engineering team.
D. Leverage CloudFormation nested stacks and stack sets for deployments. Use Amazon SNS to notify the data engineering team.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A DevOps engineer has implemented a CI/CD pipeline to deploy an AWS CloudFormation template that provisions a web application. The web application consists of an Application Load Balancer (ALB), a target group, a launch template that uses an Amazon Linux 2 AMI, an Auto Scaling group of Amazon EC2 instances, a security group, and an Amazon RDS for MySQL database. The launch template includes user data that specifies a script to install and start the application.The initial deployment of the application was successful. The DevOps engineer made changes to update the version of the application with the user data. The CI/CD pipeline has deployed a new version of the template. However, the health checks on the ALB are now failing. The health checks have marked all targets as unhealthy.During investigation, the DevOps engineer notices that the CloudFormation stack has a status of UPDATE_COMPLETE. However, when the DevOps engineer connects to one of the EC2 instances and checks /var/log/messages, the DevOps engineer notices that the Apache web server failed to start successfully because of a configuration error.How can the DevOps engineer ensure that the CloudFormation deployment will fail if the user data fails to successfully finish running?

A. Use the cfn-signal helper script to signal success or failure to CloudFormation. Use the WaitOnResourceSignals update policy within the CloudFormation template. Set an appropriate timeout for the update policy.
B. Create an Amazon CloudWatch alarm for the UnhealthyHostCount metric. Include an appropriate alarm threshold for the target group. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target to signal success or failure to CloudFormation.
C. Create a lifecycle hook on the Auto Scaling group by using the AWS::AutoScaling::LifecycleHook resource. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target to signal success or failure to CloudFormation. Set an appropriate timeout on the lifecycle hook.
D. Use the Amazon CloudWatch agent to stream the cloud-init logs. Create a subscription filter that includes an AWS Lambda function with an appropriate invocation timeout. Configure the Lambda function to use the SignalResource API operation to signal success or failure to CloudFormation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A company has a data ingestion application that runs across multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to monitor the application and consolidate access to the application. Currently, the company is running the application on Amazon EC2 instances from several Auto Scaling groups. The EC2 instances have no access to the internet because the data is sensitive. Engineers have deployed the necessary VPC endpoints. The EC2 instances run a custom AMI that is built specifically for the application.To maintain and troubleshoot the application, system administrators need the ability to log in to the EC2 instances. This access must be automated and controlled centrally. The companyâ€™s security team must receive a notification whenever the instances are accessed.Which solution will meet these requirements?

A. Create an Amazon EventBridge rule to send notifications to the security team whenever a user logs in to an EC2 instance. Use EC2 Instance Connect to log in to the instances. Deploy Auto Scaling groups by using AWS CloudFormation. Use the cfn-init helper script to deploy appropriate VPC routes for external access. Rebuild the custom AMI so that the custom AMI includes AWS Systems Manager Agent.
B. Deploy a NAT gateway and a bastion host that has internet access. Create a security group that allows incoming traffic on all the EC2 instances from the bastion host. Install AWS Systems Manager Agent on all the EC2 instances. Use Auto Scaling group lifecycle hooks for monitoring and auditing access. Use Systems Manager Session Manager to log in to the instances. Send logs to a log group in Amazon

CloudWatch Logs. Export data to Amazon S3 for auditing. Send notifications to the security team by using S3 event notifications.

C. Use EC2 Image Builder to rebuild the custom AM
D. Use AWS Systems Manager Automation to build Systems Manager Agent into the custom AM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A company uses Amazon S3 to store proprietary information. The development team creates buckets for new projects on a daily basis. The security team wants to ensure that all existing and future buckets have encryption, logging, and versioning enabled. Additionally, no buckets should ever be publicly read or write accessible.What should a DevOps engineer do to meet these requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
A DevOps engineer is researching the least expensive way to implement an image batch processing cluster on AWS. The application cannot run in Docker containers and must run on Amazon EC2. The batch job stores checkpoint data on an NFS volume and can tolerate interruptions. Configuring the cluster software from a generic EC2 Linux image takes 30 minutes.What is the MOST cost-effective solution?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A company recently migrated its legacy application from on-premises to AWS. The application is hosted on Amazon EC2 instances behind an Application Load Balancer, which is behind Amazon API Gateway. The company wants to ensure users experience minimal disruptions during any deployment of a new version of the

application. The company also wants to ensure it can quickly roll back updates if there is an issue.Which solution will meet these requirements with MINIMAL changes to the application?

A. Introduce changes as a separate environment parallel to the existing one. Configure API Gateway to use a canary release deployment to send a small subset of user traffic to the new environment.
B. Introduce changes as a separate environment parallel to the existing one. Update the applicationâ€™s DNS alias records to point to the new environment.
C. Introduce changes as a separate target group behind the existing Application Load Balancer. Configure API Gateway to route user traffic to the new target group in steps.
D. Introduce changes as a separate target group behind the existing Application Load Balancer. Configure API Gateway to route all traffic to the Application Load Balancer, which then sends the traffic to the new target group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A company is storing 100 GB of log data in .csv format in an Amazon S3 bucket. SQL developers want to query this data and generate graphs to visualize it. The SQL developers also need an efficient, automated way to store metadata from the .csv file.Which combination of steps will meet these requirements with the LEAST amount of effort? (Choose three.)

A. Filter the data through AWS X-Ray to visualize the data.
B. Filter the data through Amazon QuickSight to visualize the data.
C. Query the data with Amazon Athena.
D. Query the data with Amazon Redshift.
E. Use the AWS Glue Data Catalog as the persistent metadata store.
F. Use Amazon DynamoDB as the persistent metadata store.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A company deploys its corporate infrastructure on AWS across multiple AWS Regions and Availability Zones. The infrastructure is deployed on Amazon EC2 instances and connects with AWS IoT Greengrass devices. The company deploys additional resources on on-premises servers that are located in the corporate headquarters.The company wants to reduce the overhead involved in maintaining and updating its resources. The companyâ€™s DevOps team plans to use AWS Systems Manager to implement automated management and application of patches. The DevOps team confirms that Systems Manager is available in the Regions that the resources are deployed in. Systems Manager also is available in a Region near the corporate headquarters.Which combination of steps must the DevOps team take to implement automated patch and configuration management across the companyâ€™s EC2 instances, IoT devices, and on-premises infrastructure? (Choose three.)

A. Apply tags to all the EC2 instances, AWS IoT Greengrass devices, and on-premises servers. Use Systems Manager Session Manager to push patches to all the tagged devices.
B. Use Systems Manager Run Command to schedule patching for the EC2 instances, AWS IoT Greengrass devices, and on-premises servers.

C. Use Systems Manager Patch Manager to schedule patching for the EC2 instances, AWS IoT Greengrass devices, and on-premises servers as a Systems Manager maintenance window task.
D. Configure Amazon EventBridge to monitor Systems Manager Patch Manager for updates to patch baselines. Associate Systems Manager Run Command with the event to initiate a patch action for all EC2 instances, AWS IoT Greengrass devices, and on-premises servers.
E. Create an IAM instance profile for Systems Manager. Attach the instance profile to all the EC2 instances in the AWS account. For the AWS IoT Greengrass devices and on-premises servers, create an IAM service role for Systems Manager.
F. Generate a managed-instance activation. Use the Activation Code and Activation ID to install Systems Manager Agent (SSM Agent) on each server in the on-premises environment. Update the AWS IoT Greengrass IAM token exchange role. Use the role to deploy SSM Agent on all the IoT devices.

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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 operationally 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 cluster.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
An ecommerce company is receiving reports that its order history page is experiencing delays in reflecting the processing status of orders. The order processing system consists of an AWS Lambda function that uses reserved concurrency. The Lambda function processes order messages from an Amazon Simple Queue Service (Amazon SQS) queue and inserts processed orders into an Amazon DynamoDB table. The DynamoDB table has auto scaling enabled for read and write capacity.Which actions should a DevOps engineer take to resolve this delay? (Choose two.)

A. Check the ApproximateAgeOfOldestMessage metric for the SQS queue. Increase the Lambda function concurrency limit.
B. Check the ApproximateAgeOfOldestMessage metnc for the SQS queue Configure a redrive policy on the SQS queue.
C. Check the NumberOfMessagesSent metric for the SQS queue. Increase the SQS queue visibility timeout.
D. Check the WriteThrottleEvents metric for the DynamoDB table. Increase the maximum write capacity units (WCUs) for the table's scaling policy.

E. Check the Throttles metric for the Lambda function. Increase the Lambda function timeout.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A DevOps engineer needs to configure a blue/green deployment for an existing three-tier application. The application runs on Amazon EC2 instances and uses an Amazon RDS database. The EC2 instances run behind an Application Load Balancer (ALB) and are in an Auto Scaling group.The DevOps engineer has created a launch template and an Auto Scaling group for the blue environment. The DevOps engineer also has created a launch template and an Auto Scaling group for the green environment. Each Auto Scaling group deploys to a matching blue or green target group. The target group also specifies which software, blue or green, gets loaded on the EC2 instances. The ALB can be configured to send traffic to the blue environmentâ€™s target group or the green environmentâ€™s target group. An Amazon Route 53 record for www.example.com points to the ALB.The deployment must move traffic all at once between the software on the blue environmentâ€™s EC2 instances to the newly deployed software on the green environmentâ€™s EC2 instances.What should the DevOps engineer do to meet these requirements?

A. Start a rolling restart of the Auto Scaling group for the green environment to deploy the new software on the green environmentâ€™s EC2 instances. When the rolling restart is complete, use an AWS CLI command to update the ALB to send traffic to the green environmentâ€™s target group.
B. Use an AWS CLI command to update the ALB to send traffic to the green environmentâ€™s target group. Then start a rolling restart of the Auto Scaling group for the green environment to deploy the new software on the green environmentâ€™s EC2 instances.
C. Update the launch template to deploy the green environmentâ€™s software on the blue environmentâ€™s EC2 instances. Keep the target groups and Auto Scaling groups unchanged in both environments. Perform a rolling restart of the blue environmentâ€™s EC2 instances.
D. Start a rolling restart of the Auto Scaling group for the green environment to deploy the new software on the green environmentâ€™s EC2 instances. When the rolling restart is complete, update the Route 53 DNS to point to the green environmentâ€™s endpoint on the AL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A company is building a new pipeline by using AWS CodePipeline and AWS CodeBuild in a build account. The pipeline consists of two stages. The first stage is a CodeBuild job to build and package an AWS Lambda function. The second stage consists of deployment actions that operate on two different AWS accounts: a development environment account and a production environment account. The deployment stages use the AWS CloudFormation action that CodePipeline invokes to deploy the infrastructure that the Lambda function requires.A DevOps engineer creates the CodePipeline pipeline and configures the pipeline to encrypt build artifacts by using the AWS Key Management Service (AWS KMS) AWS managed key for Amazon S3 (the aws/s3 key). The artifacts are stored in an S3 bucket. When the pipeline runs, the CloudFormation actions fail with an access denied error.Which combination of actions must the DevOps engineer perform to resolve this error? (Choose two.)

A. Create an S3 bucket in each AWS account for the artifacts. Allow the pipeline to write to the S3 buckets. Create a CodePipeline S3 action to copy the artifacts to the S3 bucket in each AWS account. Update the CloudFormation actions to reference the artifacts S3 bucket in the production account.
B. Create a customer managed KMS key. Configure the KMS key policy to allow the IAM roles used by the

CloudFormation action to perform decrypt operations. Modify the pipeline to use the customer managed KMS key to encrypt artifacts.

C. Create an AWS managed KMS key. Configure the KMS key policy to allow the development account and the production account to perform decrypt operations. Modify the pipeline to use the KMS key to encrypt artifacts.

D. In the development account and in the production account, create an IAM role for CodePipeline. Configure the roles with permissions to perform CloudFormation operations and with permissions to retrieve and decrypt objects from the artifacts S3 bucket. In the CodePipeline account, configure the CodePipeline CloudFormation action to use the roles.

E. In the development account and in the production account, create an IAM role for CodePipeline. Configure the roles with permissions to perform CloudFormation operations and with permissions to retrieve and decrypt objects from the artifacts S3 bucket. In the CodePipeline account, modify the artifacts S3 bucket policy to allow the roles access. Configure the CodePipeline CloudFormation action to use the roles.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A company is using an organization in AWS Organizations to manage multiple AWS accounts. The companyâ €™s development team wants to use AWS Lambda functions to meet resiliency requirements and is rewriting all applications to work with Lambda functions that are deployed in a VPC. The development team is using Amazon Elastic File System (Amazon EFS) as shared storage in Account A in the organization.The company wants to continue to use Amazon EFS with Lambda. Company policy requires all serverless projects to be deployed in Account B.A DevOps engineer needs to reconfigure an existing EFS file system to allow Lambda functions to access the data through an existing EFS access point.Which combination of steps should the DevOps engineer take to meet these requirements? (Choose three.)

A. Update the EFS file system policy to provide Account B with access to mount and write to the EFS file system in Account

B. Create SCPs to set permission guardrails with fine-grained control for Amazon EF

C. Create a new EFS file system in Account

D. Update the Lambda execution roles with permission to access the VPC and the EFS file system.

E. Create a VPC peering connection to connect Account A to Account

F. Configure the Lambda functions in Account B to assume an existing IAM role in Account

Correct Answer: AADEB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A media company has several thousand Amazon EC2 instances in an AWS account. The company is using Slack and a shared email inbox for team communications and important updates. A DevOps engineer needs to send all AWS-scheduled EC2 maintenance notifications to the Slack channel and the shared inbox. The solution must include the instancesâ€™ Name and Owner tags.Which solution will meet these requirements?

A. Integrate AWS Trusted Advisor with AWS Config. Configure a custom AWS Config rule to invoke an AWS Lambda function to publish notifications to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe a Slack channel endpoint and the shared inbox to the topic.

B. Use Amazon EventBridge to monitor for AWS Health events. Configure the maintenance events to target

an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to send notifications to the Slack channel and the shared inbox.

C. Create an AWS Lambda function that sends EC2 maintenance notifications to the Slack channel and the shared inbox. Monitor EC2 health events by using Amazon CloudWatch metrics. Configure a CloudWatch alarm that invokes the Lambda function when a maintenance notification is received.

D. Configure AWS Support integration with AWS CloudTrail. Create a CloudTrail lookup event to invoke an AWS Lambda function to pass EC2 maintenance notifications to Amazon Simple Notification Service (Amazon SNS). Configure Amazon SNS to target the Slack channel and the shared inbox.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 Amazon CloudWatch Logs for CodePipeline and CodeDeploy, create an AWS Config rule to evaluate code deployment issues, and create an Amazon Simple Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.

B. Implement Amazon EventBridge for CodePipeline and CodeDeploy, create an AWS Lambda function to evaluate code deployment issues, and create an Amazon Simple Notification Service (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 Simple Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.

D. Implement Amazon EventBridge for CodePipeline and CodeDeploy, create an Amazon Inspector assessment target to evaluate code deployment issues, and create an Amazon Simple Notification Service (Amazon SNS) topic to notify stakeholders of deployment issues.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A global company manages multiple AWS accounts by using AWS Control Tower. The company hosts internal applications and public applications.Each application team in the company has its own AWS account for application hosting. The accounts are consolidated in an organization in AWS Organizations. One of the AWS Control Tower member accounts serves as a centralized DevOps account with CI/CD pipelines that application teams use to deploy applications to their respective target AWS accounts. An IAM role for deployment exists in the centralized DevOps account.An application team is attempting to deploy its application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in an application AWS account. An IAM role for deployment exists in the application AWS account. The deployment is through an AWS CodeBuild project that is set up in the centralized DevOps account. The CodeBuild project uses an IAM service role for CodeBuild. The deployment is failing with an Unauthorized error during attempts to connect to the cross-account EKS cluster from CodeBuild.Which solution will resolve this error?

A. Configure the application accountâ€™s deployment IAM role to have a trust relationship with the centralized DevOps account. Configure the trust relationship to allow the sts:AssumeRole action. Configure

the application accountâ€™s deployment IAM role to have the required access to the EKS cluster. Configure the EKS cluster aws-auth ConfigMap to map the role to the appropriate system permissions.

B. Configure the centralized DevOps accountâ€™s deployment IAM role to have a trust relationship with the application account. Configure the trust relationship to allow the sts:AssumeRole action. Configure the centralized DevOps accountâ€™s deployment IAM role to allow the required access to CodeBuild.

C. Configure the centralized DevOps accountâ€™s deployment IAM role to have a trust relationship with the application account. Configure the trust relationship to allow the sts:AssumeRoleWithSAML action. Configure the centralized DevOps accountâ€™s deployment IAM role to allow the required access to CodeBuild.

D. Configure the application accountâ€™s deployment IAM role to have a trust relationship with the AWS Control Tower management account. Configure the trust relationship to allow the sts:AssumeRole action. Configure the application accountâ€™s deployment IAM role to have the required access to the EKS cluster. Configure the EKS cluster aws-auth ConfigMap to map the role to the appropriate system permissions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A highly regulated company has a policy that DevOps engineers should not log in to their Amazon EC2 instances except in emergencies. If a DevOps engineer does log in, the security team must be notified within 15 minutes of the occurrence.Which solution will meet these requirements?

A. Install the Amazon Inspector agent on each EC2 instance. Subscribe to Amazon EventBridge notifications. Invoke an AWS Lambda function to check if a message is about user logins. If it is, send a notification to the security team using Amazon SN

B. Install the Amazon CloudWatch agent on each EC2 instance. Configure the agent to push all logs to Amazon CloudWatch Logs and set up a CloudWatch metric filter that searches for user logins. If a login is found, send a notification to the security team using Amazon SN

C. Set up AWS CloudTrail with Amazon CloudWatch Logs. Subscribe CloudWatch Logs to Amazon Kinesis. Attach AWS Lambda to Kinesis to parse and determine if a log contains a user login. If it does, send a notification to the security team using Amazon SN

D. Set up a script on each Amazon EC2 instance to push all logs to Amazon S3. Set up an S3 event to invoke an AWS Lambda function, which invokes an Amazon Athena query to run. The Athena query checks for logins and sends the output to the security team using Amazon SN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A company updated the AWS CloudFormation template for a critical business application. The stack update process failed due to an error in the updated template, and AWS CloudFormation automatically began the stack rollback process. Later, a DevOps engineer discovered that the application was still unavailable and that the stack was in the UPDATE_ROLLBACK_FAILED state.Which combination of actions should the DevOps engineer perform so that the stack rollback can complete successfully? (Choose two.)

A. Attach the AWSCloudFormationFullAccess IAM policy to the AWS CloudFormation role.

B. Automatically recover the stack resources by using AWS CloudFormation drift detection.

C. Issue a ContinueUpdateRollback command from the AWS CloudFormation console or the AWS CL

D. Manually adjust the resources to match the expectations of the stack.
E. Update the existing AWS CloudFormation stack by using the original template.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A development team manually builds an artifact locally and then places it in an Amazon S3 bucket. The application has a local cache that must be cleared when a deployment occurs. The team runs a command to do this, downloads the artifact from Amazon S3, and unzips the artifact to complete the deployment.A DevOps team wants to migrate to a CI/CD process and build in checks to stop and roll back the deployment when a failure occurs. This requires the team to track the progression of the deployment.Which combination of actions will accomplish this? (Choose three.)

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

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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:What changes should be recommended to comply with AWS security best practices? (Choose 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 â€˜db-deploy-bucketâ€™ Amazon S3 bucket, add a prebuild stage to download, then export the variables.
E. Use AWS Systems Manager run command versus scp and ssh commands directly to the instance.
F. Scramble the environment variables using XOR followed by Base64, add a section to install, and then run XOR and Base64 to the build phase.

Correct Answer: BCE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A company has a single AWS account that runs hundreds of Amazon EC2 instances in a single AWS Region. New EC2 instances are launched and terminated each hour in the account. The account also includes existing EC2 instances that have been running for longer than a week.The company's security policy requires all running EC2 instances to use an EC2 instance profile. If an EC2 instance does not have an instance profile attached, the EC2 instance must use a default instance profile that has no IAM permissions assigned.A DevOps engineer reviews the account and discovers EC2 instances that are running without an instance profile. During the review, the DevOps engineer also observes that new EC2 instances are being launched without an instance profile.Which solution will ensure that an instance profile is attached to all existing and future EC2 instances in the Region?

A. Configure an Amazon EventBridge rule that reacts to EC2 RunInstances API calls. Configure the rule to invoke an AWS Lambda function to attach the default instance profile to the EC2 instances.
B. Configure the ec2-instance-profile-attached AWS Config managed rule with a trigger type of configuration changes. Configure an automatic remediation action that invokes an AWS Systems Manager Automation runbook to attach the default instance profile to the EC2 instances.
C. Configure an Amazon EventBridge rule that reacts to EC2 StartInstances API calls. Configure the rule to invoke an AWS Systems Manager Automation runbook to attach the default instance profile to the EC2 instances
D. Configure the iam-role-managed-policy-check AWS Config managed rule with a trigger type of configuration changes. Configure an automatic remediation action that invokes an AWS Lambda function to attach the default instance profile to the EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A company has a legacy application. A DevOps engineer needs to automate the process of building the deployable artifact for the legacy application. The solution must store the deployable artifact in an existing Amazon S3 bucket for future deployments to reference.Which solution will meet these requirements in the MOST operationally efficient way?

A. Create a custom Docker image that contains all the dependencies for the legacy application. Store the custom Docker image in a new Amazon Elastic Container Registry (Amazon ECR) repository. Configure a new AWS CodeBuild project to use the custom Docker image to build the deployable artifact and to save the artifact to the S3 bucket.
B. Launch a new Amazon EC2 instance. Install all the dependencies for the legacy application on the EC2 instance. Use the EC2 instance to build the deployable artifact and to save the artifact to the S3 bucket.
C. Create a custom EC2 Image Builder image. Install all the dependencies for the legacy application on the image. Launch a new Amazon EC2 instance from the image. Use the new EC2 instance to build the deployable artifact and to save the artifact to the S3 bucket.
D. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with an AWS Fargate profile that runs in multiple Availability Zones. Create a custom Docker image that contains all the dependencies for the legacy application. Store the custom Docker image in a new Amazon Elastic Container Registry (Amazon ECR) repository. Use the custom Docker image inside the EKS cluster to build the deployable artifact and to save the artifact to the S3 bucket.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A company builds a container image in an AWS CodeBuild project by running Docker commands. After the container image is built, the CodeBuild project uploads the container image to an Amazon S3 bucket. The CodeBuild project has an IAM service role that has permissions to access the S3 bucket.A DevOps engineer needs to replace the S3 bucket with an Amazon Elastic Container Registry (Amazon ECR) repository to store the container images. The DevOps engineer creates an ECR private image repository in the same AWS Region of the CodeBuild project. The DevOps engineer adjusts the IAM service role with the permissions that are necessary to work with the new ECR repository. The DevOps engineer also places new repository information into the docker build command and the docker push command that are used in the buildspec.yml file.When the CodeBuild project runs a build job, the job fails when the job tries to access the ECR repository.Which solution will resolve the issue of failed access to the ECR repository?

A. Update the buildspec.yml file to log in to the ECR repository by using the aws ecr get-login-password AWS CLI command to obtain an authentication token. Update the docker login command to use the authentication token to access the ECR repository.
B. Add an environment variable of type SECRETS_MANAGER to the CodeBuild project. In the environment variable, include the ARN of the CodeBuild project's IAM service role. Update the buildspec.yml file to use the new environment variable to log in with the docker login command to access the ECR repository.
C. Update the ECR repository to be a public image repository. Add an ECR repository policy that allows the IAM service role to have access.
D. Update the buildspec.yml file to use the AWS CLI to assume the IAM service role for ECR operations. Add an ECR repository policy that allows the IAM service role to have access.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A company manually provisions IAM access for its employees. The company wants to replace the manual process with an automated process. The company has an existing Active Directory system configured with an external SAML 2.0 identity provider (IdP).The company wants employees to use their existing corporate credentials to access AWS. The groups from the existing Active Directory system must be available for permission management in AWS Identity and Access Management (IAM). A DevOps engineer has completed the initial configuration of AWS IAM Identity Center (AWS Single Sign-On) in the companyâ€™s AWS account.What should the DevOps engineer do next to meet the requirements?

A. Configure an external IdP as an identity source. Configure automatic provisioning of users and groups by using the SCIM protocol.
B. Configure AWS Directory Service as an identity source. Configure automatic provisioning of users and groups by using the SAML protocol.
C. Configure an AD Connector as an identity source. Configure automatic provisioning of users and groups by using the SCIM protocol.
D. Configure an external IdP as an identity source Configure automatic provisioning of users and groups by using the SAML protocol.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A company is using AWS to run digital workloads. Each application team in the company has its own AWS account for application hosting. The accounts are consolidated in an organization in AWS Organizations.The company wants to enforce security standards across the entire organization. To avoid noncompliance because of security misconfiguration, the company has enforced the use of AWS CloudFormation. A production support team can modify resources in the production environment by using the AWS Management Console to troubleshoot and resolve application-related issues.A DevOps engineer must implement a solution to identify in near real time any AWS service misconfiguration that results in noncompliance. The solution must automatically remediate the issue within 15 minutes of identification. The solution also must track noncompliant resources and events in a centralized dashboard with accurate timestamps.Which solution will meet these requirements with the LEAST development overhead?

A. Use CloudFormation drift detection to identify noncompliant resources. Use drift detection events from CloudFormation to invoke an AWS Lambda function for remediation. Configure the Lambda function to publish logs to an Amazon CloudWatch Logs log group. Configure an Amazon CloudWatch dashboard to use the log group for tracking.
B. Turn on AWS CloudTrail in the AWS accounts. Analyze CloudTrail logs by using Amazon Athena to identify noncompliant resources. Use AWS Step Functions to track query results on Athena for drift detection and to invoke an AWS Lambda function for remediation. For tracking, set up an Amazon QuickSight dashboard that uses Athena as the data source.
C. Turn on the configuration recorder in AWS Config in all the AWS accounts to identify noncompliant resources. Enable AWS Security Hub with the --no-enable-default-standards option in all the AWS accounts. Set up AWS Config managed rules and custom rules. Set up automatic remediation by using AWS Config conformance packs. For tracking, set up a dashboard on Security Hub in a designated Security Hub administrator account.
D. Turn on AWS CloudTrail in the AWS accounts. Analyze CloudTrail logs by using Amazon CloudWatch Logs to identify noncompliant resources. Use CloudWatch Logs filters for drift detection. Use Amazon EventBridge to invoke the Lambda function for remediation. Stream filtered CloudWatch logs to Amazon OpenSearch Service. Set up a dashboard on OpenSearch Service for tracking.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A company uses AWS Organizations to manage its AWS accounts. The organization root has an OU that is named Environments. The Environments OU has two child OUs that are named Development and Production, respectively.The Environments OU and the child OUs have the default FullAWSAccess policy in place. A DevOps engineer plans to remove the FullAWSAccess policy from the Development OU and replace the policy with a policy that allows all actions on Amazon EC2 resources.What will be the outcome of this policy replacement?

A. All users in the Development OU will be allowed all API actions on all resources.
B. All users in the Development OU will be allowed all API actions on EC2 resources. All other API actions will be denied.
C. All users in the Development OU will be denied all API actions on all resources.
D. All users in the Development OU will be denied all API actions on EC2 resources. All other API actions will be allowed.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 41
A company is examining its disaster recovery capability and wants the ability to switch over its daily operations to a secondary AWS Region. The company uses AWS CodeCommit as a source control tool in the primary Region.A DevOps engineer must provide the capability for the company to develop code in the secondary Region. If the company needs to use the secondary Region, developers can add an additional remote URL to their local Git configuration.Which solution will meet these requirements?

A. Create a CodeCommit repository in the secondary Region. Create an AWS CodeBuild project to perform a Git mirror operation of the primary Region's CodeCommit repository to the secondary Region's CodeCommit repository. Create an AWS Lambda function that invokes the CodeBuild project. Create an Amazon EventBridge rule that reacts to merge events in the primary Region's CodeCommit repository. Configure the EventBridge rule to invoke the Lambda function.
B. Create an Amazon S3 bucket in the secondary Region. Create an AWS Fargate task to perform a Git mirror operation of the primary Region's CodeCommit repository and copy the result to the S3 bucket. Create an AWS Lambda function that initiates the Fargate task. Create an Amazon EventBridge rule that reacts to merge events in the CodeCommit repository. Configure the EventBridge rule to invoke the Lambda function.
C. Create an AWS CodeArtifact repository in the secondary Region. Create an AWS CodePipeline pipeline that uses the primary Regionâ€™s CodeCommit repository for the source action. Create a cross-Region stage in the pipeline that packages the CodeCommit repository contents and stores the contents in the CodeArtifact repository when a pull request is merged into the CodeCommit repository.
D. Create an AWS Cloud9 environment and a CodeCommit repository in the secondary Region. Configure the primary Region's CodeCommit repository as a remote repository in the AWS Cloud9 environment. Connect the secondary Region's CodeCommit repository to the AWS Cloud9 environment.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A DevOps team is merging code revisions for an application that uses an Amazon RDS Multi-AZ DB cluster for its production database. The DevOps team uses continuous integration to periodically verify that the application works. The DevOps team needs to test the changes before the changes are deployed to the production database.Which solution will meet these requirements?

A. Use a buildspec file in AWS CodeBuild to restore the DB cluster from a snapshot of the production database, run integration tests, and drop the restored database after verification.
B. Deploy the application to production. Configure an audit log of data control language (DCL) operations to capture database activities to perform if verification fails.
C. Create a snapshot of the DB cluster before deploying the application. Use the Update requires:Replacement property on the DB instance in AWS CloudFormation to deploy the application and apply the changes.
D. Ensure that the DB cluster is a Multi-AZ deployment. Deploy the application with the updates. Fail over to the standby instance if verification fails.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A company manages a multi-tenant environment in its VPC and has configured Amazon GuardDuty for the corresponding AWS account. The company sends all GuardDuty findings to AWS Security Hub.Traffic from suspicious sources is generating a large number of findings. A DevOps engineer needs to implement a solution to automatically deny traffic across the entire VPC when GuardDuty discovers a new suspicious source.Which solution will meet these requirements?

A. Create a GuardDuty threat list. Configure GuardDuty to reference the list. Create an AWS Lambda function that will update the threat list. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.
B. Configure an AWS WAF web ACL that includes a custom rule group. Create an AWS Lambda function that will create a block rule in the custom rule group. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.
C. Configure a firewall in AWS Network Firewall. Create an AWS Lambda function that will create a Drop action rule in the firewall policy. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.
D. Create an AWS Lambda function that will create a GuardDuty suppression rule. Configure the Lambda function to run in response to new Security Hub findings that come from GuardDuty.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A company uses AWS Secrets Manager to store a set of sensitive API keys that an AWS Lambda function uses. When the Lambda function is invoked the Lambda function retrieves the API keys and makes an API call to an external service. The Secrets Manager secret is encrypted with the default AWS Key Management Service (AWS KMS) key.A DevOps engineer needs to update the infrastructure to ensure that only the Lambda functionâ€™s execution role can access the values in Secrets Manager. The solution must apply the principle of least privilege.Which combination of steps will meet these requirements? (Choose two.)

A. Update the default KMS key for Secrets Manager to allow only the Lambda functionâ€™s execution role to decrypt
B. Create a KMS customer managed key that trusts Secrets Manager and allows the Lambda function's execution role to decrypt. Update Secrets Manager to use the new customer managed key
C. Create a KMS customer managed key that trusts Secrets Manager and allows the account's root principal to decrypt. Update Secrets Manager to use the new customer managed key
D. Ensure that the Lambda functionâ€™s execution role has the KMS permissions scoped on the resource level. Configure the permissions so that the KMS key can encrypt the Secrets Manager secret
E. Remove all KMS permissions from the Lambda functionâ€™s execution role

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A company's DevOps engineer is creating an AWS Lambda function to process notifications from an Amazon Simple Notification Service (Amazon SNS) topic. The Lambda function will process the notification messages

and will write the contents of the notification messages to an Amazon RDS Multi-AZ DB instance.During testing, a database administrator accidentally shut down the DB instance. While the database was down the company lost several of the SNS notification messages that were delivered during that time.The DevOps engineer needs to prevent the loss of notification messages in the future.Which solutions will meet this requirement? (Choose two.)

A. Replace the RDS Multi-AZ DB instance with an Amazon DynamoDB table.
B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination of the Lambda function.
C. Configure an Amazon Simple Queue Service (Amazon SQS) dead-letter queue for the SNS topic.
D. Subscribe an Amazon Simple Queue Service (Amazon SQS) queue to the SNS topic. Configure the Lambda function to process messages from the SQS queue.
E. Replace the SNS topic with an Amazon EventBridge event bus. Configure an EventBridge rule on the new event bus to invoke the Lambda function for each event.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A DevOps engineer is building a continuous deployment pipeline for a serverless application that uses AWS Lambda functions. The company wants to reduce the customer impact of an unsuccessful deployment. The company also wants to monitor for issues.Which deploy stage configuration will meet these requirements?

A. Use an AWS Serverless Application Model (AWS SAM) template to define the serverless application. Use AWS CodeDeploy to deploy the Lambda functions with the Canary10Percent15Minutes Deployment Preference Type. Use Amazon CloudWatch alarms to monitor the health of the functions.
B. Use AWS CloudFormation to publish a new stack update, and include Amazon CloudWatch alarms on all resources. Set up an AWS CodePipeline approval action for a developer to verify and approve the AWS CloudFormation change set.
C. Use AWS CloudFormation to publish a new version on every stack update, and include Amazon CloudWatch alarms on all resources. Use the RoutingConfig property of the AWS::Lambda::Alias resource to update the traffic routing during the stack update.
D. Use AWS CodeBuild to add sample event payloads for testing to the Lambda functions. Publish a new version of the functions, and include Amazon CloudWatch alarms. Update the production alias to point to the new version. Configure rollbacks to occur when an alarm is in the ALARM state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A company has an application that runs on Amazon EC2 instances. The company uses an AWS CodePipeline pipeline to deploy the application into multiple AWS Regions. The pipeline is configured with a stage for each Region. Each stage contains an AWS CloudFormation action for each Region.When the pipeline deploys the application to a Region, the company wants to confirm that the application is in a healthy state before the pipeline moves on to the next Region. Amazon Route 53 record sets are configured for the application in each Region. A DevOps engineer creates a Route 53 health check that is based on an Amazon CloudWatch alarm for each Region where the application is deployed.What should the DevOps engineer do next to meet the requirements?

A. Create an AWS Step Functions workflow to check the state of the CloudWatch alarm. Configure the Step Functions workflow to exit with an error if the alarm is in the ALARM state. Create a new stage in the pipeline between each Region deployment stage. In each new stage, include an action to invoke the Step Functions workflow.
B. Configure an AWS CodeDeploy application to deploy a CloudFormation template with automatic rollback. Configure the CloudWatch alarm as the instance health check for the CodeDeploy application. Remove the CloudFormation actions from the pipeline. Create a CodeDeploy action in the pipeline stage for each Region.
C. Create a new pipeline stage for each Region where the application is deployed. Configure a CloudWatch alarm action for the new stage to check the state of the CloudWatch alarm and to exit with an error if the alarm is in the ALARM state
D. Configure the CloudWatch agent on the EC2 instances to report the application status to the Route 53 health check. Create a new pipeline stage for each Region where the application is deployed. Configure a CloudWatch alarm action to exit with an error if the CloudWatch alarm is in the ALARM state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A company plans to use Amazon CloudWatch to monitor its Amazon EC2 instances. The company needs to stop EC2 instances when the average of the NetworkPacketsIn metric is less than 5 for at least 3 hours in a 12-hour time window. The company must evaluate the metric every hour. The EC2 instances must continue to run if there is missing data for the NetworkPacketsIn metric during the evaluation period.A DevOps engineer creates a CloudWatch alarm for the NetworkPacketsIn metric. The DevOps engineer configures a threshold value of 5 and an evaluation period of 1 hour.Which set of additional actions should the DevOps engineer take to meet these requirements?

A. Configure the Datapoints to Alarm value to be 3 out of 12. Configure the alarm to treat missing data as breaching the threshold. Add an AWS Systems Manager action to stop the instance when the alarm enters the ALARM state.
B. Configure the Datapoints to Alarm value to be 3 out of 12. Configure the alarm to treat missing data as not breaching the threshold. Add an EC2 action to stop the instance when the alarm enters the ALARM state.
C. Configure the Datapoints to Alarm value to be 9 out of 12. Configure the alarm to treat missing data as breaching the threshold. Add an EC2 action to stop the instance when the alarm enters the ALARM state.
D. Configure the Datapoints to Alarm value to be 9 out of 12. Configure the alarm to treat missing data as not breaching the threshold. Add an AWS Systems Manager action to stop the instance when the alarm enters the ALARM state.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
A company manages 500 AWS accounts that are in an organization in AWS Organizations. The company discovers many unattached Amazon Elastic Block Store (Amazon EBS) volumes in all the accounts. The company wants to automatically tag the unattached EBS volumes for investigation.A DevOps engineer needs to deploy an AWS Lambda function to all the AWS accounts. The Lambda function must run every 30 minutes to tag all the EBS volumes that have been unattached for a period of 7 days or more.Which solution will meet these requirements in the MOST operationally efficient manner?

A. Configure a delegated administrator account for the organization. Create an AWS CloudFormation template that contains the Lambda function. Use CloudFormation StackSets to deploy the CloudFormation template from the delegated administrator account to all the member accounts in the organization. Create an Amazon EventBridge event bus in the delegated administrator account to invoke the Lambda function in each member account every 30 minutes.
B. Create a cross-account IAM role in the organization's member accounts. Attach the AWSLambda_FullAccess policy and the AWSCloudFormationFullAccess policy to the role. Create an AWS CloudFormation template that contains the Lambda function and an Amazon EventBridge scheduled rule to invoke the Lambda function every 30 minutes. Create a custom script in the organizationâ€™s management account that assumes the role and deploys the CloudFormation template to the member accounts.
C. Configure a delegated administrator account for the organization. Create an AWS CloudFormation template that contains the Lambda function and an Amazon EventBridge scheduled rule to invoke the Lambda function every 30 minutes. Use CloudFormation StackSets to deploy the CloudFormation template from the delegated administrator account to all the member accounts in the organization
D. Create a cross-account IAM role in the organization's member accounts. Attach the AmazonS3FullAccess policy and the AWSCodeDeployDeployerAccess policy to the role. Use AWS CodeDeploy to assume the role to deploy the Lambda function from the organization's management account. Configure an Amazon EventBridge scheduled rule in the member accounts to invoke the Lambda function every 30 minutes.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A company's production environment uses an AWS CodeDeploy blue/green deployment to deploy an application. The deployment incudes Amazon EC2 Auto Scaling groups that launch instances that run Amazon Linux 2.A working appspec.yml file exists in the code repository and contains the following text:A DevOps engineer needs to ensure that a script downloads and installs a license file onto the instances before the replacement instances start to handle request traffic. The DevOps engineer adds a hooks section to the appspec.yml file.Which hook should the DevOps engineer use to run the script that downloads and installs the license file?

A. AfterBlockTraffic
B. BeforeBlockTraffic
C. BeforeInstall
D. DownloadBundle

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A company has an application that includes AWS Lambda functions. The Lambda functions run Python code that is stored in an AWS CodeCommit repository. The company has recently experienced failures in the production environment because of an error in the Python code. An engineer has written unit tests for the Lambda functions to help avoid releasing any future defects into the production environment.The company's DevOps team needs to implement a solution to integrate the unit tests into an existing AWS CodePipeline pipeline. The solution must produce reports about the unit tests for the company to view.Which solution will meet these requirements?

A. Associate the CodeCommit repository with Amazon CodeGuru Reviewer. Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create a buildspec.yml file in the CodeCommit repository. In the buildspec yml file, define the actions to run a CodeGuru review.
B. Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create a CodeBuild report group. Create a buildspec.yml file in the CodeCommit repository. In the buildspec.yml file, define the actions to run the unit tests with an output of JUNITXML in the build phase section. Configure the test reports to be uploaded to the new CodeBuild report group.
C. Create a new AWS CodeArtifact repository. Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create an appspec.yml file in the original CodeCommit repository. In the appspec.yml file, define the actions to run the unit tests with an output of CUCUMBERJSON in the build phase section. Configure the tests reports to be sent to the new CodeArtifact repository.
D. Create a new AWS CodeBuild project. In the CodePipeline pipeline, configure a test stage that uses the new CodeBuild project. Create a new Amazon S3 bucket. Create a buildspec.yml file in the CodeCommit repository. In the buildspec yml file, define the actions to run the unit tests with an output of HTML in the phases section. In the reports section, upload the test reports to the S3 bucket.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A company manages multiple AWS accounts in AWS Organizations. The companyâ€™s security policy states that AWS account root user credentials for member accounts must not be used. The company monitors access to the root user credentials.A recent alert shows that the root user in a member account launched an Amazon EC2 instance. A DevOps engineer must create an SCP at the organization's root level that will prevent the root user in member accounts from making any AWS service API calls.Which SCP will meet these requirements?

A.
B.
C.
D.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A company uses AWS and has a VPC that contains critical compute infrastructure with predictable traffic patterns. The company has configured VPC flow logs that are published to a log group in Amazon CloudWatch Logs.The company's DevOps team needs to configure a monitoring solution for the VPC flow logs to identify anomalies in network traffic to the VPC over time. If the monitoring solution detects an anomaly, the company needs the ability to initiate a response to the anomaly.How should the DevOps team configure the monitoring solution to meet these requirements?

A. Create an Amazon Kinesis data stream. Subscribe the log group to the data stream. Configure Amazon Kinesis Data Analytics to detect log anomalies in the data stream. Create an AWS Lambda function to use as the output of the data stream. Configure the Lambda function to write to the default Amazon EventBridge event bus in the event of an anomaly finding.

B. Create an Amazon Kinesis Data Firehose delivery stream that delivers events to an Amazon S3 bucket. Subscribe the log group to the delivery stream. Configure Amazon Lookout for Metrics to monitor the data in the S3 bucket for anomalies. Create an AWS Lambda function to run in response to Lookout for Metrics anomaly findings. Configure the Lambda function to publish to the default Amazon EventBridge event bus.
C. Create an AWS Lambda function to detect anomalies. Configure the Lambda function to publish an event to the default Amazon EventBridge event bus if the Lambda function detects an anomaly. Subscribe the Lambda function to the log group.
D. Create an Amazon Kinesis data stream. Subscribe the log group to the data stream. Create an AWS Lambda function to detect log anomalies. Configure the Lambda function to write to the default Amazon EventBridge event bus if the Lambda function detects an anomaly. Set the Lambda function as the processor for the data stream.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
AnyCompany is using AWS Organizations to create and manage multiple AWS accounts. AnyCompany recently acquired a smaller company, Example Corp. During the acquisition process, Example Corp's single AWS account joined AnyCompany's management account through an Organizations invitation. AnyCompany moved the new member account under an OU that is dedicated to Example Corp.AnyCompany's DevOps engineer has an IAM user that assumes a role that is named OrganizationAccountAccessRole to access member accounts. This role is configured with a full access policy. When the DevOps engineer tries to use the AWS Management Console to assume the role in Example Corp's new member account, the DevOps engineer receives the following error message: "Invalid information in one or more fields. Check your information or contact your administrator."Which solution will give the DevOps engineer access to the new member account?

A. In the management account, grant the DevOps engineer's IAM user permission to assume the OrganizationAccountAccessRole IAM role in the new member account.
B. In the management account, create a new SC
C. In the new member account, create a new IAM role that is named OrganizationAccountAccessRole. Attach the AdministratorAccess AWS managed policy to the role. In the role's trust policy, grant the management account permission to assume the role.
D. In the new member account, edit the trust policy for the OrganizationAccountAccessRole IAM role. Grant the management account permission to assume the role.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A DevOps engineer is designing an application that integrates with a legacy REST API. The application has an AWS Lambda function that reads records from an Amazon Kinesis data stream. The Lambda function sends the records to the legacy REST API.Approximately 10% of the records that the Lambda function sends from the Kinesis data stream have data errors and must be processed manually. The Lambda function event source configuration has an Amazon Simple Queue Service (Amazon SQS) dead-letter queue as an on-failure destination. The DevOps engineer has configured the Lambda function to process records in batches and has implemented retries in case of failure.During testing, the DevOps engineer notices that the dead-letter queue contains many records that have no data errors and that already have been processed by the legacy REST API. The DevOps engineer needs to configure the Lambda function's event source options to reduce the number of errorless records that are sent to the dead-letter queue.Which solution will meet these

requirements?

A. Increase the retry attempts.
B. Configure the setting to split the batch when an error occurs.
C. Increase the concurrent batches per shard.
D. Decrease the maximum age of record.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
To run an application, a DevOps engineer launches an Amazon EC2 instance 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 allow only outbound traffic to the artifact

repository. Remove the security group rule once the install is complete.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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:â€¢ Separate environment pipelines for testing and productionâ€¢ Automatic deployment that occurs for test environments onlyWhich 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 the 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A DevOps engineer wants to find a solution to migrate an application from on premises to AWS. The application is running on Linux and needs to run on specific versions of Apache Tomcat, HAProxy, and Varnish Cache to function properly. The application's operating system-level parameters require tuning. The solution must include a way to automate the deployment of new application versions. The infrastructure should be scalable and faulty servers should be replaced automatically.Which solution should the DevOps engineer use?

A. Upload the application as a Docker image that contains all the necessary software to Amazon EC
B. Upload the application code to an AWS CodeCommit repository with a saved configuration file to configure and install the software. Create an AWS Elastic Beanstalk web server tier and a load balanced-type environment that uses the Tomcat solution stack. Create an AWS CodePipeline pipeline that uses CodeCommit as a source and Elastic Beanstalk as a deployment provider.
C. Upload the application code to an AWS CodeCommit repository with a set of .ebextensions files to configure and install the software. Create an AWS Elastic Beanstalk worker tier environment that uses the Tomcat solution stack. Create an AWS CodePipeline pipeline that uses CodeCommit as a source and Elastic Beanstalk as a deployment provider.
D. Upload the application code to an AWS CodeCommit repository with an appspec.yml file to configure and

install the necessary software. Create an AWS CodeDeploy deployment group associated with an Amazon EC2 Auto Scaling group. Create an AWS CodePipeline pipeline that uses CodeCommit as a source and CodeDeploy as a deployment provider.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A security team is concerned that a developer can unintentionally attach an Elastic IP address to an Amazon EC2 instance in production. No developer should be allowed to attach an Elastic IP address to an instance. The security team must be notified if any production server has an Elastic IP address at any time.How can this task be automated?

A. Use Amazon Athena to query AWS CloudTrail logs to check for any associate-address attempts. Create an AWS Lambda function to disassociate the Elastic IP address from the instance, and alert the security team.
B. Attach an IAM policy to the developers' IAM group to deny associate-address permissions. Create a custom AWS Config rule to check whether an Elastic IP address is associated with any instance tagged as production, and alert the security team.
C. Ensure that all IAM groups 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 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A company is using AWS Organizations to create separate AWS accounts for each of its departments. The company needs to automate the following tasks:â€¢ Update the Linux AMIs with new patches periodically and generate a golden imageâ€¢ Install a new version of Chef agents in the golden image, if availableâ€¢ Provide the newly generated AMIs to the department's accountsWhich solution meets these requirements with the LEAST management overhead?

A. Write a script to launch an Amazon EC2 instance from the previous golden image. Apply the patch updates. Install the new version of the Chef agent, generate a new golden image, and then modify the AMI permissions to share only the new image with the department's accounts.
B. Use Amazon EC2 Image Builder to create an image pipeline that consists of the base Linux AMI and components to install the Chef agent. Use AWS Resource Access Manager to share EC2 Image Builder images with the department's accounts.
C. Use an AWS Systems Manager Automation runbook to update the Linux AMI by using the previous image. Provide the URL for the script that will update the Chef agent. Use AWS Organizations to replace the previous golden image in the department's accounts.
D. Use Amazon EC2 Image Builder to create an image pipeline that consists of the base Linux AMI and components to install the Chef agent. Create a parameter in AWS Systems Manager Parameter Store to store the new AMI ID that can be referenced by the department's accounts.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A company has a mission-critical application on AWS that uses automatic scaling. The company wants the deployment lifecycle to meet the following parameters:â€¢ The application must be deployed one instance at a time to ensure the remaining fleet continues to serve traffic.â€¢ The application is CPU intensive and must be closely monitored.â€¢ The deployment must automatically roll back if the CPU utilization of the deployment instance exceeds 85%.Which solution will meet these requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 main 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 main 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 main 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 main branch for production code, and create a testing branch for code deployed to testing. Have developers use each branch for developing in each environment.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A DevOps engineer notices that all Amazon EC2 instances running behind an Application Load Balancer in an Auto Scaling group are failing to respond to user requests. The EC2 instances are also failing target group HTTP health checks.Upon inspection, the engineer notices the application process was not running in any EC2 instances. There are a significant number of out of memory messages in the system logs. The engineer needs to improve the resilience of the application to cope with a potential application memory leak. Monitoring and notifications should be enabled to alert when there is an issue.Which combination of actions will meet these requirements? (Choose two.)

A. Change the Auto Scaling configuration to replace the instances when they fail the load balancer's health checks.
B. Change the target group health check HealthCheckIntervalSeconds parameter to reduce the interval between health checks.
C. Change the target group health checks from HTTP to TCP to check if the port where the application is listening is reachable.
D. Enable the available memory consumption metric within the Amazon CloudWatch dashboard for the entire Auto Scaling group. Create an alarm when the memory utilization is high. Associate an Amazon SNS topic to the alarm to receive notifications when the alarm goes off.
E. Use the Amazon CloudWatch agent to collect the memory utilization of the EC2 instances in the Auto Scaling group. Create an alarm when the memory utilization is high and associate an Amazon SNS topic to receive a notification.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A company manages AWS accounts for application teams in AWS Control Tower. Individual application teams are responsible for securing their respective AWS accounts.A DevOps engineer needs to enable Amazon GuardDuty for all AWS accounts in which the application teams have not already enabled GuardDuty. The DevOps engineer is using AWS CloudFormation StackSets from the AWS Control Tower management account.How should the DevOps engineer configure the CloudFormation template to prevent failure during the StackSets deployment?

A. Create a CloudFormation custom resource that invokes an AWS Lambda function. Configure the Lambda function to conditionally enable GuardDuty if GuardDuty is not already enabled in the accounts.
B. Use the Conditions section of the CloudFormation template to enable GuardDuty in accounts where GuardDuty is not already enabled.
C. Use the CloudFormation Fn::GetAtt intrinsic function to check whether GuardDuty is already enabled. If GuardDuty is not already enabled, use the Resources section of the CloudFormation template to enable GuardDuty.
D. Manually discover the list of AWS account IDs where GuardDuty is not enabled. Use the CloudFormation Fn::ImportValue intrinsic function to import the list of account IDs into the CloudFormation template to skip deployment for the listed AWS accounts.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A development team is using AWS CodeCommit to version control application code and AWS CodePipeline to orchestrate software deployments. The team has decided to use a remote main branch as the trigger for the pipeline to integrate code changes. A developer has pushed code changes to the CodeCommit repository, but noticed that the pipeline had no reaction, even after 10 minutes.Which of the following actions should be taken to troubleshoot this issue?

A. Check that an Amazon EventBridge rule has been created for the main branch to trigger the pipeline.

B. Check that the CodePipeline service role has permission to access the CodeCommit repository.
C. Check that the developerâ€™s IAM role has permission to push to the CodeCommit repository.
D. Check to see if the pipeline failed to start because of CodeCommit errors in Amazon CloudWatch Logs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A company has an AWS Control Tower landing zone. The company's DevOps team creates a workload OU. A development OU and a production OU are nested under the workload OU. The company grants users full access to the company's AWS accounts to deploy applications.The DevOps team needs to allow only a specific management IAM role to manage the IAM roles and policies of any AWS accounts in only the production OU.Which combination of steps will meet these requirements? (Choose two.)

A. Create an SCP that denies full access with a condition to exclude the management IAM role for the organization root.
B. Ensure that the FullAWSAccess SCP is applied at the organization root.
C. Create an SCP that allows IAM related actions. Attach the SCP to the development O
D. Create an SCP that denies IAM related actions with a condition to exclude the management IAM role. Attach the SCP to the workload O
E. Create an SCP that denies IAM related actions with a condition to exclude the management IAM role. Attach the SCP to the production O

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A company hired a penetration tester to simulate an internal security breach. The tester performed port scans on the company's Amazon EC2 instances. The company's security measures did not detect the port scans.The company needs a solution that automatically provides notification when port scans are performed on EC2 instances. The company creates and subscribes to an Amazon Simple Notification Service (Amazon SNS) topic.What should the company do next to meet the requirement?

A. Ensure that Amazon GuardDuty is enabled. Create an Amazon CloudWatch alarm for detected EC2 and port scan findings. Connect the alarm to the SNS topic.
B. Ensure that Amazon Inspector is enabled. Create an Amazon EventBridge event for detected network reachability findings that indicate port scans. Connect the event to the SNS topic.
C. Ensure that Amazon Inspector is enabled. Create an Amazon EventBridge event for detected CVEs that cause open port vulnerabilities. Connect the event to the SNS topic.
D. Ensure that AWS CloudTrail is enabled. Create an AWS Lambda function to analyze the CloudTrail logs for unusual amounts of traffic from an IP address range. Connect the Lambda function to the SNS topic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A company runs applications in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster uses an Application Load Balancer to route traffic to the applications that run in the cluster.A new application that was migrated to the EKS cluster is performing poorly. All the other applications in the EKS cluster maintain appropriate operation. The new application scales out horizontally to the preconfigured maximum number of pods immediately upon deployment, before any user traffic routes to the web application.Which solution will resolve the scaling behavior of the web application in the EKS cluster?

A. Implement the Horizontal Pod Autoscaler in the EKS cluster.
B. Implement the Vertical Pod Autoscaler in the EKS cluster.
C. Implement the Cluster Autoscaler.
D. Implement the AWS Load Balancer Controller in the EKS cluster.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A company has an AWS Control Tower landing zone that manages its organization in AWS Organizations. The company created an OU structure that is based on the company's requirements. The company's DevOps team has established the core accounts for the solution and an account for all centralized AWS CloudFormation and AWS Service Catalog solutions.The company wants to offer a series of customizations that an account can request through AWS Control Tower.Which combination of steps will meet these requirements? (Choose three.)

A. Enable trusted access for CloudFormation with Organizations by using service-managed permissions.
B. Create an IAM role that is named AWSControlTowerBlueprintAccess. Configure the role with a trust policy that allows the AWSControlTowerAdmin role in the management account to assume the role. Attach the AWSServiceCatalogAdminFullAccess IAM policy to the AWSControlTowerBlueprintAccess role.
C. Create a Service Catalog product for each CloudFormation template.
D. Create a CloudFormation stack set for each CloudFormation template. Enable automatic deployment for each stack set. Create a CloudFormation stack instance that targets specific OUs.
E. Deploy the Customizations for AWS Control Tower (CfCT) CloudFormation stack.
F. Create a CloudFormation template that contains the resources for each customization.

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A company runs a workload on Amazon EC2 instances. The company needs a control that requires the use of Instance Metadata Service Version 2 (IMDSv2) on all EC2 instances in the AWS account. If an EC2 instance does not prevent the use of Instance Metadata Service Version 1 (IMDSv1), the EC2 instance must be terminated.Which solution will meet these requirements?

A. Set up AWS Config in the account. Use a managed rule to check EC2 instances. Configure the rule to remediate the findings by using AWS Systems Manager Automation to terminate the instance.
B. Create a permissions boundary that prevents the ec2:RunInstance action if the ec2:MetadataHttpTokens condition key is not set to a value of required. Attach the permissions boundary to the IAM role that was

used to launch the instance.

C. Set up Amazon Inspector in the account. Configure Amazon Inspector to activate deep inspection for EC2 instances. Create an Amazon EventBridge rule for an Inspector2 finding. Set an AWS Lambda function as the target to terminate the instance.

D. Create an Amazon EventBridge rule for the EC2 instance launch successful event. Send the event to an AWS Lambda function to inspect the EC2 metadata and to terminate the instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company builds an application that uses an Application Load Balancer in front of Amazon EC2 instances that are in an Auto Scaling group. The application is stateless. The Auto Scaling group uses a custom AMI that is fully prebuilt. The EC2 instances do not have a custom bootstrapping process.The AMI that the Auto Scaling group uses was recently deleted. The Auto Scaling group's scaling activities show failures because the AMI ID does not exist.Which combination of steps should a DevOps engineer take to meet these requirements? (Choose three.)

A. Create a new launch template that uses the new AM
B. Update the Auto Scaling group to use the new launch template.
C. Reduce the Auto Scaling group's desired capacity to 0.
D. Increase the Auto Scaling group's desired capacity by 1.
E. Create a new AMI from a running EC2 instance in the Auto Scaling group.
F. Create a new AMI by copying the most recent public AMI of the operating system that the EC2 instances use.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A company deploys a web application on Amazon EC2 instances that are behind an Application Load Balancer (ALB). The company stores the application code in an AWS CodeCommit repository. When code is merged to the main branch, an AWS Lambda function invokes an AWS CodeBuild project. The CodeBuild project packages the code, stores the packaged code in AWS CodeArtifact, and invokes AWS Systems Manager Run Command to deploy the packaged code to the EC2 instances.Previous deployments have resulted in defects, EC2 instances that are not running the latest version of the packaged code, and inconsistencies between instances.Which combination of actions should a DevOps engineer take to implement a more reliable deployment solution? (Choose two.)

A. Create a pipeline in AWS CodePipeline that uses the CodeCommit repository as a source provider. Configure pipeline stages that run the CodeBuild project in parallel to build and test the application. In the pipeline, pass the CodeBuild project output artifact to an AWS CodeDeploy action.
B. Create a pipeline in AWS CodePipeline that uses the CodeCommit repository as a source provider. Create separate pipeline stages that run a CodeBuild project to build and then test the application. In the pipeline, pass the CodeBuild project output artifact to an AWS CodeDeploy action.
C. Create an AWS CodeDeploy application and a deployment group to deploy the packaged code to the EC2 instances. Configure the ALB for the deployment group.
D. Create individual Lambda functions that use AWS CodeDeploy instead of Systems Manager to run build,

test, and deploy actions.

E. Create an Amazon S3 bucket. Modify the CodeBuild project to store the packages in the S3 bucket instead of in CodeArtifact. Use deploy actions in CodeDeploy to deploy the artifact to the EC2 instances.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A company uses an organization in AWS Organizations to manage its AWS accounts. The company's automation account contains a CI/CD pipeline that creates and configures new AWS accounts.The company has a group of internal service teams that provide services to accounts in the organization. The service teams operate out of a set of services accounts. The service teams want to receive an AWS CloudTrail event in their services accounts when the CreateAccount API call creates a new account.How should the company share this CloudTrail event with the service accounts?

A. Create an Amazon EventBridge rule in the automation account to send account creation events to the default event bus in the services accounts. Update the default event bus in the services accounts to allow events from the automation account.
B. Create a custom Amazon EventBridge event bus in the services accounts. Update the custom event bus to allow events from the automation account. Create an EventBridge rule in the services account that directly listens to CloudTrail events from the automation account.
C. Create a custom Amazon EventBridge event bus in the automation account and the services accounts. Create an EventBridge rule and policy that connects the custom event buses that are in the automation account and the services accounts.
D. Create a custom Amazon EventBridge event bus in the automation account. Create an EventBridge rule and policy that connects the custom event bus to the default event buses in the services accounts.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A DevOps engineer is building a solution that uses Amazon Simple Queue Service (Amazon SQS) standard queues. The solution also includes an AWS Lambda function and an Amazon DynamoDB table. The Lambda function pulls content from an SQS queue event source and writes the content to the DynamoDB table.The solution must maximize the scalability of Lambda and must prevent successfully processed SQS messages from being processed multiple times.Which solution will meet these requirements?

A. Decrease the batch window to 1 second when configuring the Lambda function's event source mapping.
B. Decrease the batch size to 1 when configuring the Lambda function's event source mapping.
C. Include the ReportBatchItemFailures value in the FunctionResponseTypes list in the Lambda function's event source mapping.
D. Set the queue visibility timeout on the Lambda function's event source mapping to account for invocation throttling of the Lambda function.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A company has a new AWS account that teams will use to deploy various applications. The teams will create many Amazon S3 buckets for application-specific purposes and to store AWS CloudTrail logs. The company has enabled Amazon Macie for the account.A DevOps engineer needs to optimize the Macie costs for the account without compromising the account's functionality.Which solutions will meet these requirements? (Choose two.)

A. Exclude S3 buckets that contain CloudTrail logs from automated discovery.
B. Exclude S3 buckets that have public read access from automated discovery.
C. Configure scheduled daily discovery jobs for all S3 buckets in the account.
D. Configure discovery jobs to include S3 objects based on the last modified criterion.
E. Configure discovery jobs to include S3 objects that are tagged as production only.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A company's developers use Amazon EC2 instances as remote workstations. The company is concerned that users can create or modify EC2 security groups to allow unrestricted inbound access.A DevOps engineer needs to develop a solution to detect when users create unrestricted security group rules. The solution must detect changes to security group rules in near real time, remove unrestricted rules, and send email notifications to the security team. The DevOps engineer has created an AWS Lambda function that checks for security group ID from input, removes rules that grant unrestricted access, and sends notifications through Amazon Simple Notification Service (Amazon SNS).What should the DevOps engineer do next to meet the requirements?

A. Configure the Lambda function to be invoked by the SNS topic. Create an AWS CloudTrail subscription for the SNS topic. Configure a subscription filter for security group modification events.
B. Create an Amazon EventBridge scheduled rule to invoke the Lambda function. Define a schedule pattern that runs the Lambda function every hour.
C. Create an Amazon EventBridge event rule that has the default event bus as the source. Define the ruleâ €™s event pattern to match EC2 security group creation and modification events. Configure the rule to invoke the Lambda function.
D. Create an Amazon EventBridge custom event bus that subscribes to events from all AWS services. Configure the Lambda function to be invoked by the custom event bus.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A company uses an organization in AWS Organizations to manage its AWS accounts. The company recently acquired another company that has standalone AWS accounts. The acquiring company's DevOps team needs to consolidate the administration of the AWS accounts for both companies and retain full administrative control of the accounts. The DevOps team also needs to collect and group findings across all the accounts to implement and maintain a security posture.Which combination of steps should the DevOps team take to meet these requirements? (Choose two.)

A. Invite the acquired company's AWS accounts to join the organization. Create an SCP that has full administrative privileges. Attach the SCP to the management account.
B. Invite the acquired company's AWS accounts to join the organization. Create the OrganizationAccountAccessRole IAM role in the invited accounts. Grant permission to the management account to assume the role.
C. Use AWS Security Hub to collect and group findings across all accounts. Use Security Hub to automatically detect new accounts as the accounts are added to the organization.
D. Use AWS Firewall Manager to collect and group findings across all accounts. Enable all features for the organization. Designate an account in the organization as the delegated administrator account for Firewall Manager.
E. Use Amazon Inspector to collect and group findings across all accounts. Designate an account in the organization as the delegated administrator account for Amazon Inspector.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
A company has an application and a CI/CD pipeline. The CI/CD pipeline consists of an AWS CodePipeline pipeline and an AWS CodeBuild project. The CodeBuild project runs tests against the application as part of the build process and outputs a test report. The company must keep the test reports for 90 days.Which solution will meet these requirements?

A. Add a new stage in the CodePipeline pipeline after the stage that contains the CodeBuild project. Create an Amazon S3 bucket to store the reports. Configure an S3 deploy action type in the new CodePipeline stage with the appropriate path and format for the reports.
B. Add a report group in the CodeBuild project buildspec file with the appropriate path and format for the reports. Create an Amazon S3 bucket to store the reports. Configure an Amazon EventBridge rule that invokes an AWS Lambda function to copy the reports to the S3 bucket when a build is completed. Create an S3 Lifecycle rule to expire the objects after 90 days.
C. Add a new stage in the CodePipeline pipeline. Configure a test action type with the appropriate path and format for the reports. Configure the report expiration time to be 90 days in the CodeBuild project buildspec file.
D. Add a report group in the CodeBuild project buildspec file with the appropriate path and format for the reports. Create an Amazon S3 bucket to store the reports. Configure the report group as an artifact in the CodeBuild project buildspec file. Configure the S3 bucket as the artifact destination. Set the object expiration to 90 days.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A company uses an Amazon API Gateway regional REST API to host its application API. The REST API has a custom domain. The REST API's default endpoint is deactivated.The company's internal teams consume the API. The company wants to use mutual TLS between the API and the internal teams as an additional layer of authentication.Which combination of steps will meet these requirements? (Choose two.)

A. Use AWS Certificate Manager (ACM) to create a private certificate authority (CA). Provision a client certificate that is signed by the private C
B. Provision a client certificate that is signed by a public certificate authority (CA). Import the certificate into

AWS Certificate Manager (ACM).

C. Upload the provisioned client certificate to an Amazon S3 bucket. Configure the API Gateway mutual TLS to use the client certificate that is stored in the S3 bucket as the trust store.

D. Upload the provisioned client certificate private key to an Amazon S3 bucket. Configure the API Gateway mutual TLS to use the private key that is stored in the S3 bucket as the trust store.

E. Upload the root private certificate authority (CA) certificate to an Amazon S3 bucket. Configure the API Gateway mutual TLS to use the private CA certificate that is stored in the S3 bucket as the trust store.

Correct Answer: AAE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A company uses AWS Directory Service for Microsoft Active Directory as its identity provider (IdP). The company requires all infrastructure to be defined and deployed by AWS CloudFormation.A DevOps engineer needs to create a fleet of Windows-based Amazon EC2 instances to host an application. The DevOps engineer has created a CloudFormation template that contains an EC2 launch template, IAM role, EC2 security group, and EC2 Auto Scaling group. The DevOps engineer must implement a solution that joins all EC2 instances to the domain of the AWS Managed Microsoft AD directory.Which solution will meet these requirements with the MOST operational efficiency?

A. In the CloudFormation template, create an AWS::SSM::Document resource that joins the EC2 instance to the AWS Managed Microsoft AD domain by using the parameters for the existing directory. Update the launch template to include the SSMAssociation property to use the new SSM document. Attach the AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess AWS managed policies to the IAM role that the EC2 instances use.

B. In the CloudFormation template, update the launch template to include specific tags that propagate on launch. Create an AWS::SSM::Association resource to associate the AWS-JoinDirectoryServiceDomain Automation runbook with the EC2 instances that have the specified tags. Define the required parameters to join the AWS Managed Microsoft AD directory. Attach the AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess AWS managed policies to the IAM role that the EC2 instances use.

C. Store the existing AWS Managed Microsoft AD domain connection details in AWS Secrets Manager. In the CloudFormation template, create an AWS::SSM::Association resource to associate the AWS-CreateManagedWindowsInstanceWithApproval Automation runbook with the EC2 Auto Scaling group. Pass the ARNs for the parameters from Secrets Manager to join the domain. Attach the AmazonSSMDirectoryServiceAccess and SecretsManagerReadWrite AWS managed policies to the IAM role that the EC2 instances use.

D. Store the existing AWS Managed Microsoft AD domain administrator credentials in AWS Secrets Manager. In the CloudFormation template, update the EC2 launch template to include user data. Configure the user data to pull the administrator credentials from Secrets Manager and to join the AWS Managed Microsoft AD domain. Attach the AmazonSSMManagedInstanceCore and SecretsManagerReadWrite AWS managed policies to the IAM role that the EC2 instances use.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
A company uses AWS Organizations to manage its AWS accounts. The company has a root OU that has a child OU. The root OU has an SCP that allows all actions on all resources. The child OU has an SCP that allows all actions for Amazon DynamoDB and AWS Lambda, and denies all other actions.The company has an AWS account that is named vendor-data in the child OU. A DevOps engineer has an IAM user that is attached

to the Administrator Access IAM policy in the vendor-data account. The DevOps engineer attempts to launch an Amazon EC2 instance in the vendor-data account but receives an access denied error.Which change should the DevOps engineer make to launch the EC2 instance in the vendor-data account?

A. Attach the AmazonEC2FullAccess IAM policy to the IAM user.
B. Create a new SCP that allows all actions for Amazon EC2. Attach the SCP to the vendor-data account.
C. Update the SCP in the child OU to allow all actions for Amazon EC2.
D. Create a new SCP that allows all actions for Amazon EC2. Attach the SCP to the root O

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A company's security policies require the use of security hardened AMIs in production environments. A DevOps engineer has used EC2 Image Builder to create a pipeline that builds the AMIs on a recurring schedule.The DevOps engineer needs to update the launch templates of the company's Auto Scaling groups. The Auto Scaling groups must use the newest AMIs during the launch of Amazon EC2 instances.Which solution will meet these requirements with the MOST operational efficiency?

A. Configure an Amazon EventBridge rule to receive new AMI events from Image Builder. Target an AWS Systems Manager Run Command document that updates the launch templates of the Auto Scaling groups with the newest AMI I
B. Configure an Amazon EventBridge rule to receive new AMI events from Image Builder. Target an AWS Lambda function that updates the launch templates of the Auto Scaling groups with the newest AMI I
C. Configure the launch template to use a value from AWS Systems Manager Parameter Store for the AMI I
D. Configure the Image Builder pipeline to update the Parameter Store value with the newest AMI I

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A company has configured an Amazon S3 event source on an AWS Lambda function. The company needs the Lambda function to run when a new object is created or an existing object is modified in a particular S3 bucket. The Lambda function will use the S3 bucket name and the S3 object key of the incoming event to read the contents of the created or modified S3 object. The Lambda function will parse the contents and save the parsed contents to an Amazon DynamoDB table.The Lambda function's execution role has permissions to read from the S3 bucket and to write to the DynamoDB table. During testing, a DevOps engineer discovers that the Lambda function does not run when objects are added to the S3 bucket or when existing objects are modified.Which solution will resolve this problem?

A. Increase the memory of the Lambda function to give the function the ability to process large files from the S3 bucket.
B. Create a resource policy on the Lambda function to grant Amazon S3 the permission to invoke the Lambda function for the S3 bucket.
C. Configure an Amazon Simple Queue Service (Amazon SQS) queue as an OnFailure destination for the Lambda function.
D. Provision space in the /tmp folder of the Lambda function to give the function the ability to process large files from the S3 bucket.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
A company has deployed a critical application in two AWS Regions. The application uses an Application Load Balancer (ALB) in both Regions. The company has Amazon Route 53 alias DNS records for both ALBs.The company uses Amazon Route 53 Application Recovery Controller to ensure that the application can fail over between the two Regions. The Route 53 ARC configuration includes a routing control for both Regions. The company uses Route 53 ARC to perform quarterly disaster recovery (DR) tests.During the most recent DR test, a DevOps engineer accidentally turned off both routing controls. The company needs to ensure that at least one routing control is turned on at all times.Which solution will meet these requirements?

A. In Route 53 ARC, create a new assertion safety rule. Apply the assertion safety rule to the two routing controls. Configure the rule with the ATLEAST type with a threshold of 1.
B. In Route 53 ARC, create a new gating safety rule. Apply the assertion safety rule to the two routing controls. Configure the rule with the OR type with a threshold of 1.
C. In Route 53 ARC, create a new resource set. Configure the resource set with an AWS::Route53::HealthCheck resource type. Specify the ARNs of the two routing controls as the target resource. Create a new readiness check for the resource set.
D. In Route 53 ARC, create a new resource set. Configure the resource set with an AWS::Route53RecoveryReadiness::DNSTargetResource resource type. Add the domain names of the two Route 53 alias DNS records as the target resource. Create a new readiness check for the resource set.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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 DynamoDUse 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 for MySQL DB instance. Generate a report by querying the RDS instance and exporting the query results to a CSV text file.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A DevOps engineer is planning to deploy a Ruby-based application to production. The application needs to interact with an Amazon RDS for MySQL database and should have automatic scaling and high availability. The stored data in the database is critical and should persist regardless of the state of the application stack.The DevOps engineer needs to set up an automated deployment strategy for the application with automatic rollbacks. The solution also must alert the application team when a deployment fails.Which combination of steps will meet these requirements? (Choose three.)

A. Deploy the application on AWS Elastic Beanstalk. Deploy an Amazon RDS for MySQL DB instance as part of the Elastic Beanstalk configuration.
B. Deploy the application on AWS Elastic Beanstalk. Deploy a separate Amazon RDS for MySQL DB instance outside of Elastic Beanstalk.
C. Configure a notification email address that alerts the application team in the AWS Elastic Beanstalk configuration.
D. Configure an Amazon EventBridge rule to monitor AWS Health events. Use an Amazon Simple Notification Service (Amazon SNS) topic as a target to alert the application team.
E. Use the immutable deployment method to deploy new application versions.
F. Use the rolling deployment method to deploy new application versions.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A DevOps engineer is creating an AWS CloudFormation template to deploy a web service. The web service will run on Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). The DevOps engineer must ensure that the service can accept requests from clients that have IPv6 addresses.What should the DevOps engineer do with the CloudFormation template so that IPv6 clients can access the web service?

A. Add an IPv6 CIDR block to the VPC and the private subnet for the EC2 instances. Create route table entries for the IPv6 network, use EC2 instance types that support IPv6, and assign IPv6 addresses to each EC2 instance.
B. 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 ALB, and associate the target group with the AL
C. Replace the ALB with a Network Load Balancer (NLB). Add an IPv6 CIDR block to the VPC and subnets for the NLB, and assign the NLB an IPv6 Elastic IP address.
D. Add an IPv6 CIDR block to the VPC and subnets for the AL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A company is using AWS CodePipeline to deploy an application. According to a new guideline, a member of the company's security team must sign off on any application changes before the changes are deployed into production. The approval must be recorded and retained.Which combination of actions will meet these requirements? (Choose two.)

A. Configure CodePipeline to write actions to Amazon CloudWatch Logs.
B. Configure CodePipeline to write actions to an Amazon S3 bucket at the end of each pipeline stage.
C. Create an AWS CloudTrail trail to deliver logs to Amazon S3.
D. Create a CodePipeline custom action to invoke an AWS Lambda function for approval. Create a policy that gives the security team access to manage CodePipeline custom actions.
E. Create a CodePipeline manual approval action before the deployment step. Create a policy that grants the security team access to approve manual approval stages.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A company requires its internal business teams to launch resources through pre-approved AWS CloudFormation templates only. The security team requires automated monitoring when resources drift from their expected state.Which strategy should be used to meet these requirements?

A. Allow users to deploy CloudFormation stacks using a CloudFormation service role only. Use CloudFormation drift detection to detect when resources have drifted from their expected state.
B. Allow users to deploy CloudFormation stacks using a CloudFormation service role only. Use AWS Config rules to detect when resources have drifted from their expected state.
C. Allow users to deploy CloudFormation stacks using AWS Service Catalog only. Enforce the use of a launch constraint. Use AWS Config rules to detect when resources have drifted from their expected state.
D. Allow users to deploy CloudFormation stacks using AWS Service Catalog only. Enforce the use of a template constraint. Use Amazon EventBridge notifications to detect when resources have drifted from their expected state.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A company has multiple development groups working in a single shared AWS account. The senior manager of the groups wants to be alerted via a third-party API call when the creation of resources approaches the service limits for the account.Which solution will accomplish this with the LEAST amount of development effort?

A. Create an Amazon EventBridge rule that runs periodically and targets an AWS Lambda function. Within the Lambda function, evaluate the current state of the AWS environment and compare deployed resource values to resource limits on the account. Notify the senior manager if the account is approaching a service limit.
B. Deploy an AWS Lambda function that refreshes AWS Trusted Advisor checks, and configure an Amazon EventBridge rule to run the Lambda function periodically. Create another EventBridge rule with an event pattern matching Trusted Advisor events and a target Lambda function. In the target Lambda function,

notify the senior manager.

C. Deploy an AWS Lambda function that refreshes AWS Health Dashboard checks, and configure an Amazon EventBridge rule to run the Lambda function periodically. Create another EventBridge rule with an event pattern matching Health Dashboard events and a target Lambda function. In the target Lambda function, notify the senior manager.

D. Add an AWS Config custom rule that runs periodically, checks the AWS service limit status, and streams notifications to an Amazon Simple Notification Service (Amazon SNS) topic. Deploy an AWS Lambda function that notifies the senior manager, and subscribe the Lambda function to the SNS topic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A DevOps engineer is setting up a container-based architecture. The engineer has decided to use AWS CloudFormation to automatically provision an Amazon ECS cluster and an Amazon EC2 Auto Scaling group to launch the EC2 container instances. After successfully creating the CloudFormation stack, the engineer noticed that, even though the ECS cluster and the EC2 instances were created successfully and the stack finished the creation, the EC2 instances were associating with a different cluster.How should the DevOps engineer update the CloudFormation template to resolve this issue?

A. Reference the EC2 instances in the AWS::ECS::Cluster resource and reference the ECS cluster in the AWS::ECS::Service resource.

B. Reference the ECS cluster in the AWS::AutoScaling::LaunchConfiguration resource of the UserData property.

C. Reference the ECS cluster in the AWS::EC2::Instance resource of the UserData property.

D. Reference the ECS cluster in the AWS::CloudFormation::CustomResource resource to trigger an AWS Lambda function that registers the EC2 instances with the appropriate ECS cluster.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A DevOps engineer is implementing governance controls for a company that requires its infrastructure to be housed within the United States. The engineer must restrict which AWS Regions can be used, and ensure an alert is sent as soon as possible if any activity outside the governance policy takes place. The controls should be automatically enabled on any new Region outside the United States (US).Which combination of actions will meet these requirements? (Choose two.)

A. Create an AWS Organizations SCP that denies access to all non-global services in non-US Regions. Attach the policy to the root of the organization.

B. Configure AWS CloudTrail to send logs to Amazon CloudWatch Logs and enable it for all Regions. Use a CloudWatch Logs metric filter to send an alert on any service activity in non-US Regions.

C. Use an AWS Lambda function that checks for AWS service activity and deploy it to all Regions. Write an Amazon EventBridge rule that runs the Lambda function every hour, sending an alert if activity is found in a non-US Region.

D. Use an AWS Lambda function to query Amazon Inspector to look for service activity in non-US Regions and send alerts if any activity is found.

E. Write an SCP using the aws:RequestedRegion condition key limiting access to US Regions. Apply the

policy to all users, groups, and roles.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A company sells products through an ecommerce web application. The company wants a dashboard that shows a pie chart of product transaction details. The company wants to integrate the dashboard with the company's existing Amazon CloudWatch dashboards.Which solution will meet these requirements with the MOST operational efficiency?

A. Update the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction. Use CloudWatch Logs Insights to query the log group and to visualize the results in a pie chart format. Attach the results to the desired CloudWatch dashboard.
B. Update the ecommerce application to emit a JSON object to an Amazon S3 bucket for each processed transaction. Use Amazon Athena to query the S3 bucket and to visualize the results in a pie chart format. Export the results from Athena. Attach the results to the desired CloudWatch dashboard.
C. Update the ecommerce application to use AWS X-Ray for instrumentation. Create a new X-Ray subsegment. Add an annotation for each processed transaction. Use X-Ray traces to query the data and to visualize the results in a pie chart format. Attach the results to the desired CloudWatch dashboard.
D. Update the ecommerce application to emit a JSON object to a CloudWatch log group for each processed transaction. Create an AWS Lambda function to aggregate and write the results to Amazon DynamoD

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A company is launching an application. The application must use only approved AWS services. The account that runs the application was created less than 1 year ago and is assigned to an AWS Organizations OU.The company needs to create a new Organizations account structure. The account structure must have an appropriate SCP that supports the use of only services that are currently active in the AWS account. The company will use AWS Identity and Access Management (IAM) Access Analyzer in the solution.Which solution will meet these requirements?

A. Create an SCP that allows the services that IAM Access Analyzer identifies. Create an OU for the account. Move the account into the new O
B. Create an SCP that denies the services that IAM Access Analyzer identifies. Create an OU for the account. Move the account into the new O
C. Create an SCP that allows the services that IAM Access Analyzer identifies. Attach the new SCP to the organization's root.
D. Create an SCP that allows the services that IAM Access Analyzer identifies. Create an OU for the account. Move the account into the new O

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A company has multiple development teams in different business units that work in a shared single AWS account. All Amazon EC2 resources that are created in the account must include tags that specify who created the resources. The tagging must occur within the first hour of resource creation.A DevOps engineer needs to add tags to the created resources that include the user ID that created the resource and the cost center ID. The DevOps engineer configures an AWS Lambda function with the cost center mappings to tag the resources. The DevOps engineer also sets up AWS CloudTrail in the AWS account. An Amazon S3 bucket stores the CloudTrail event logs.Which solution will meet the tagging requirements?

A. Create an S3 event notification on the S3 bucket to invoke the Lambda function for s3:ObjectTagging:Put events. Enable bucket versioning on the S3 bucket.
B. Enable server access logging on the S3 bucket. Create an S3 event notification on the S3 bucket for s3:ObjectTagging:* events.
C. Create a recurring hourly Amazon EventBridge scheduled rule that invokes the Lambda function. Modify the Lambda function to read the logs from the S3 bucket.
D. Create an Amazon EventBridge rule that uses Amazon EC2 as the event source. Configure the rule to match events delivered by CloudTrail. Configure the rule to target the Lambda function.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A company runs an application for multiple environments in a single AWS account. An AWS CodePipeline pipeline uses a development Amazon Elastic Container Service (Amazon ECS) cluster to test an image for the application from an Amazon Elastic Container Registry (Amazon ECR) repository. The pipeline promotes the image to a production ECS cluster.The company needs to move the production cluster into a separate AWS account in the same AWS Region. The production cluster must be able to download the images over a private connection.Which solution will meet these requirements?

A. Use Amazon ECR VPC endpoints and an Amazon S3 gateway endpoint. In the separate AWS account, create an ECR repository. Set the repository policy to allow the production ECS tasks to pull images from the main AWS account. Configure the production ECS task execution role to have permission to download the image from the ECR repository.
B. Set a repository policy on the production ECR repository in the main AWS account. Configure the repository policy to allow the production ECS tasks in the separate AWS account to pull images from the main account. Configure the production ECS task execution role to have permission to download the image from the ECR repository.
C. Configure ECR private image replication in the main AWS account. Activate cross-account replication. Define the destination account ID of the separate AWS account.
D. Use Amazon ECR VPC endpoints and an Amazon S3 gateway endpoint. Set a repository policy on the production ECR repository in the main AWS account. Configure the repository policy to allow the production ECS tasks in the separate AWS account to pull images from the main account. Configure the production ECS task execution role to have permission to download the image from the ECR repository.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100

A company needs to ensure that flow logs remain configured for all existing and new VPCs in its AWS account. The company uses an AWS CloudFormation stack to manage its VPCs. The company needs a solution that will work for any VPCs that any IAM user creates.Which solution will meet these requirements?

A. Add the AWS::EC2::FlowLog resource to the CloudFormation stack that creates the VPCs.
B. Create an organization in AWS Organizations. Add the company's AWS account to the organization. Create an SCP to prevent users from modifying VPC flow logs.
C. Turn on AWS Config. Create an AWS Config rule to check whether VPC flow logs are turned on. Configure automatic remediation to turn on VPC flow logs.
D. Create an IAM policy to deny the use of API calls for VPC flow logs. Attach the IAM policy to all IAM users.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A company uses AWS Organizations and AWS Control Tower to manage all the company's AWS accounts. The company uses the Enterprise Support plan.A DevOps engineer is using Account Factory for Terraform (AFT) to provision new accounts. When new accounts are provisioned, the DevOps engineer notices that the support plan for the new accounts is set to the Basic Support plan. The DevOps engineer needs to implement a solution to provision the new accounts with the Enterprise Support plan.Which solution will meet these requirements?

A. Use an AWS Config conformance pack to deploy the account-part-of-organizations AWS Config rule and to automatically remediate any noncompliant accounts.
B. Create an AWS Lambda function to create a ticket for AWS Support to add the account to the Enterprise Support plan. Grant the Lambda function the support:ResolveCase permission.
C. Add an additional value to the control_tower_parameters input to set the AWSEnterpriseSupport parameter as the organization's management account number.
D. Set the aft_feature_enterprise_support feature flag to True in the AFT deployment input configuration. Redeploy AFT and apply the changes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A company's application teams use AWS CodeCommit repositories for their applications. The application teams have repositories in multiple AWS accounts. All accounts are in an organization in AWS Organizations.Each application team uses AWS IAM Identity Center (AWS Single Sign-On) configured with an external IdP to assume a developer IAM role. The developer role allows the application teams to use Git to work with the code in the repositories.A security audit reveals that the application teams can modify the main branch in any repository. A DevOps engineer must implement a solution that allows the application teams to modify the main branch of only the repositories that they manage.Which combination of steps will meet these requirements? (Choose three.)

A. Update the SAML assertion to pass the user's team name. Update the IAM role's trust policy to add an access-team session tag that has the team name.
B. Create an approval rule template for each team in the Organizations management account. Associate the template with all the repositories. Add the developer role ARN as an approver.
C. Create an approval rule template for each account. Associate the template with all repositories. Add the

"aws:ResourceTag/access-team": "$;{aws:PrincipalTag/access-team}" condition to the approval rule template.

D. For each CodeCommit repository, add an access-team tag that has the value set to the name of the associated team.
E. Attach an SCP to the accounts. Include the following statement:
F. Create an IAM permissions boundary in each account. Include the following statement:

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A company uses AWS WAF to protect its cloud infrastructure. A DevOps engineer needs to give an operations team the ability to analyze log messages from AWS WAF. The operations team needs to be able to create alarms for specific patterns in the log output.Which solution will meet these requirements with the LEAST operational overhead?

A. Create an Amazon CloudWatch Logs log group. Configure the appropriate AWS WAF web ACL to send log messages to the log group. Instruct the operations team to create CloudWatch metric filters.
B. Create an Amazon OpenSearch Service cluster and appropriate indexes. Configure an Amazon Kinesis Data Firehose delivery stream to stream log data to the indexes. Use OpenSearch Dashboards to create filters and widgets.
C. Create an Amazon S3 bucket for the log output. Configure AWS WAF to send log outputs to the S3 bucket. Instruct the operations team to create AWS Lambda functions that detect each desired log message pattern. Configure the Lambda functions to publish to an Amazon Simple Notification Service (Amazon SNS) topic.
D. Create an Amazon S3 bucket for the log output. Configure AWS WAF to send log outputs to the S3 bucket. Use Amazon Athena to create an external table definition that fits the log message pattern. Instruct the operations team to write SQL queries and to create Amazon CloudWatch metric filters for the Athena queries.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A software team is using AWS CodePipeline to automate its Java application release pipeline. The pipeline consists of a source stage, then a build stage, and then a deploy stage. Each stage contains a single action that has a runOrder value of 1.The team wants to integrate unit tests into the existing release pipeline. The team needs a solution that deploys only the code changes that pass all unit tests.Which solution will meet these requirements?

A. Modify the build stage. Add a test action that has a runOrder value of 1. Use AWS CodeDeploy as the action provider to run unit tests.
B. Modify the build stage. Add a test action that has a runOrder value of 2. Use AWS CodeBuild as the action provider to run unit tests.
C. Modify the deploy stage. Add a test action that has a runOrder value of 1. Use AWS CodeDeploy as the action provider to run unit tests.
D. Modify the deploy stage. Add a test action that has a runOrder value of 2. Use AWS CodeBuild as the action provider to run unit tests.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A company uses an organization in AWS Organizations to manage several AWS accounts that the company's developers use. The company requires all data to be encrypted in transit.Multiple Amazon S3 buckets that were created in developer accounts allow unencrypted connections. A DevOps engineer must enforce encryption of data in transit for all existing S3 buckets that are created in accounts in the organization.Which solution will meet these requirements?

A. Use AWS CloudFormation StackSets to deploy an AWS Network Firewall firewall to each account. Route all outbound requests from the AWS environment through the firewall. Deploy a policy to block access to all outbound requests on port 80.
B. Use AWS CloudFormation StackSets to deploy an AWS Network Firewall firewall to each account. Route all inbound requests to the AWS environment through the firewall. Deploy a policy to block access to all inbound requests on port 80.
C. Turn on AWS Config for the organization. Deploy a conformance pack that uses the s3-bucket-ssl-requests-only managed rule and an AWS Systems Manager Automation runbook. Use a runbook that adds a bucket policy statement to deny access to an S3 bucket when the value of the aws:SecureTransport condition key is false.
D. Turn on AWS Config for the organization. Deploy a conformance pack that uses the s3-bucket-ssl-requests-only managed rule and an AWS Systems Manager Automation runbook. Use a runbook that adds a bucket policy statement to deny access to an S3 bucket when the value of the s3:x-amz-server-side-encryption-aws-kms-key-id condition key is null.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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:What changes should the engineer make to achieve a policy of least permission? (Choose three.)

A. Add the following conditional expression:
B. Change "Resource": "*"to "Resource": "arn:aws:ec2:*:*:instance/*"
C. Add the following conditional expression:
D. Add the following conditional expression:
E. Change "Action": "ec2:*"to "Action": "ec2:StopInstances"
F. Add the following conditional expression:

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A company is developing an application that will generate log events. The log events consist of five distinct metrics every one tenth of a second and produce a large amount of data.The company needs to configure the application to write the logs to Amazon Timestream. The company will configure a daily query against the Timestream table.Which combination of steps will meet these requirements with the FASTEST query performance? (Choose three.)

A. Use batch writes to write multiple log events in a single write operation.
B. Write each log event as a single write operation.
C. Treat each log as a single-measure record.
D. Treat each log as a multi-measure record.
E. Configure the memory store retention period to be longer than the magnetic store retention period.
F. Configure the memory store retention period to be shorter than the magnetic store retention period.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A DevOps engineer has created an AWS CloudFormation template that deploys an application on Amazon EC2 instances. The EC2 instances run Amazon Linux. The application is deployed to the EC2 instances by using shell scripts that contain user data. The EC2 instances have an IAM instance profile that has an IAM role with the AmazonSSMManagedinstanceCore managed policy attached.The DevOps engineer has modified the user data in the CloudFormation template to install a new version of the application. The engineer has also applied the stack update. However, the application was not updated on the running EC2 instances. The engineer needs to ensure that the changes to the application are installed on the running EC2 instances.Which combination of steps will meet these requirements? (Choose two.)

A. Configure the user data content to use the Multipurpose Internet Mail Extensions (MIME) multipart format. Set the scripts-user parameter to always in the text/cloud-config section.
B. Refactor the user data commands to use the cfn-init helper script. Update the user data to install and configure the cfn-hup and cfn-init helper scripts to monitor and apply the metadata changes.
C. Configure an EC2 launch template for the EC2 instances. Create a new EC2 Auto Scaling group. Associate the Auto Scaling group with the EC2 launch template. Use the AutoScalingScheduledAction update policy for the Auto Scaling group.
D. Refactor the user data commands to use an AWS Systems Manager document (SSM document). Add an AWS CLI command in the user data to use Systems Manager Run Command to apply the SSM document to the EC2 instances.
E. Refactor the user data command to use an AWS Systems Manager document (SSM document). Use Systems Manager State Manager to create an association between the SSM document and the EC2 instances.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
A company is refactoring applications to use AWS. The company identifies an internal web application that needs to make Amazon S3 API calls in a specific AWS account.The company wants to use its existing identity provider (IdP) auth.company.com for authentication. The IdP supports only OpenID Connect (OIDC). A DevOps engineer needs to secure the web application's access to the AWS account.Which combination of

steps will meet these requirements? (Choose three.)

A. Configure AWS IAM Identity Center (AWS Single Sign-On). Configure an Id
B. Create an IAM IdP by using the provider URL, audience, and signature from the existing I
C. Create an IAM role that has a policy that allows the necessary S3 actions. Configure the role's trust policy to allow the OIDC IP to assume the role if the sts.amazon.com:aud context key is appid_from_idp.
D. Create an IAM role that has a policy that allows the necessary S3 actions. Configure the role's trust policy to allow the OIDC IP to assume the role if the auth.company.com:aud context key is appid_from_idp.
E. Configure the web application to use the AssumeRoleWithWebIdentity API operation to retrieve temporary credentials. Use the temporary credentials to make the S3 API calls.
F. Configure the web application to use the GetFederationToken API operation to retrieve temporary credentials. Use the temporary credentials to make the S3 API calls.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A company uses Amazon RDS for all databases in its AWS accounts. The company uses AWS Control Tower to build a landing zone that has an audit and logging account. All databases must be encrypted at rest for compliance reasons. The company's security engineer needs to receive notification about any noncompliant databases that are in the companyâ€™s accounts.Which solution will meet these requirements with the MOST operational efficiency?

A. Use AWS Control Tower to activate the optional detective control (guardrail) to determine whether the RDS storage is encrypted. Create an Amazon Simple Notification Service (Amazon SNS) topic in the company's audit account. Create an Amazon EventBridge rule to filter noncompliant events from the AWS Control Tower control (guardrail) to notify the SNS topic. Subscribe the security engineer's email address to the SNS topic.
B. Use AWS CloudFormation StackSets to deploy AWS Lambda functions to every account. Write the Lambda function code to determine whether the RDS storage is encrypted in the account the function is deployed to. Send the findings as an Amazon CloudWatch metric to the management account. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create a CloudWatch alarm that notifies the SNS topic when metric thresholds are met. Subscribe the security engineer's email address to the SNS topic.
C. Create a custom AWS Config rule in every account to determine whether the RDS storage is encrypted. Create an Amazon Simple Notification Service (Amazon SNS) topic in the audit account. Create an Amazon EventBidge rule to filter noncompliant events from the AWS Control Tower control (guardrail) to notify the SNS topic. Subscribe the security engineer's email address to the SNS topic.
D. Launch an Amazon C2 instance. Run an hourly cron job by using the AWS CLI to determine whether the RDS storage is encrypted in each AWS account. Store the results in an RDS database. Notify the security engineer by sending email messages from the EC2 instance when noncompliance is detected

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A company is migrating from its on-premises data center to AWS. The company currently uses a custom on-premises CI/CD pipeline solution to build and package software.The company wants its software packages and dependent public repositories to be available in AWS CodeArtifact to facilitate the creation of application-specific pipelines.Which combination of steps should the company take to update the CI/CD pipeline solution

and to configure CodeArtifact with the LEAST operational overhead? (Choose two.)

A. Update the C1ICD pipeline to create a VM image that contains newly packaged software. Use AWS Import/ Export to make the VM image available as an Amazon EC2 AM
B. Create an AWS Identity and Access Management Roles Anywhere trust anchor. Create an IAM role that allows CodeArtifact actions and that has a trust relationship on the trust anchor. Update the on-premises CI/CD pipeline to assume the new IAM role and to publish the packages to CodeArtifact.
C. Create a new Amazon S3 bucket. Generate a presigned URL that allows the PutObject request. Update the on-premises CI/CD pipeline to use the presigned URL to publish the packages from the on-premises location to the S3 bucket. Create an AWS Lambda function that runs when packages are created in the bucket through a put command. Configure the Lambda function to publish the packages to CodeArtifact.
D. For each public repository, create a CodeArutact repository that is configured with an external connection. Configure the dependent repositories as upstream public repositories.
E. Create a Codeartitact repository that is configured with a set of external connections to the public repositories. Configure the external connections to be downstream of the repository.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A company provides an application to customers. The application has an Amazon API Gateway REST API that invokes an AWS Lambda function. On initialization, the Lambda function loads a large amount of data from an Amazon DynamoDB table. The data load process results in long cold-start times of 8-10 seconds. The DynamoDB table has DynamoDB Accelerator (DAX) configured.Customers report that the application intermittently takes a long time to respond to requests. The application receives thousands of requests throughout the day. In the middle of the day, the application experiences 10 times more requests than at any other time of the day. Near the end of the day, the application's request volume decreases to 10% of its normal total.A DevOps engineer needs to reduce the latency of the Lambda function at all times of the day.Which solution will meet these requirements?

A. Configure provisioned concurrency on the Lambda function with a concurrency value of 1. Delete the DAX cluster for the DynamoDB table.
B. Configure reserved concurrency on the Lambda function with a concurrency value of 0.
C. Configure provisioned concurrency on the Lambda function. Configure AWS Application Auto Scaling on the Lambda function with provisioned concurrency values set to a minimum of 1 and a maximum of 100.
D. Configure reserved concurrency on the Lambda function. Configure AWS Application Auto Scaling on the API Gateway API with a reserved concurrency maximum value of 100.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A company's DevOps engineer uses AWS Systems Manager to perform maintenance tasks during maintenance windows. The company has a few Amazon EC2 instances that require a restart after notifications from AWS Health. The DevOps engineer needs to implement an automated solution to remediate these notifications. The DevOps engineer creates an Amazon EventBridge rule.How should the DevOps engineer configure the EventBridge rule to meet these requirements?

A. Configure an event source of AWS Health, a service of EC2. and an event type that indicates instance

maintenance. Target a Systems Manager document to restart the EC2 instance.

B. Configure an event source of Systems Manager and an event type that indicates a maintenance window. Target a Systems Manager document to restart the EC2 instance.

C. Configure an event source of AWS Health, a service of EC2, and an event type that indicates instance maintenance. Target a newly created AWS Lambda function that registers an automation task to restart the EC2 instance during a maintenance window.

D. Configure an event source of EC2 and an event type that indicates instance maintenance. Target a newly created AWS Lambda function that registers an automation task to restart the EC2 instance during a maintenance window.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
A DevOps team uses AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy to deploy an application. The application is a REST API that uses AWS Lambda functions and Amazon API Gateway. Recent deployments have introduced errors that have affected many customers.The DevOps team needs a solution that reverts to the most recent stable version of the application when an error is detected. The solution must affect the fewest customers possible.Which solution will meet these requirements with the MOST operational efficiency?

A. Set the deployment configuration in CodeDeploy to LambdaAllAtOnce. Configure automatic rollbacks on the deployment group. Create an Amazon CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway. Configure the deployment group to roll back when the number of alarms meets the alarm threshold.

B. Set the deployment configuration in CodeDeploy to LambdaCanary10Percent10Minutes. Configure automatic rollbacks on the deployment group. Create an Amazon CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway. Configure the deployment group to roll back when the number of alarms meets the alarm threshold.

C. Set the deployment configuration in CodeDeploy to LambdaAllAtOnce. Configure manual rollbacks on the deployment group. Create an Amazon Simple Notification Service (Amazon SNS) topic to send notifications every time a deployment fails. Configure the SNS topic to invoke a new Lambda function that stops the current deployment and starts the most recent successful deployment.

D. Set the deployment configuration in CodeDeploy to LambdaCanary10Percent10Minutes. Configure manual rollbacks on the deployment group. Create a metric filter on an Amazon CloudWatch log group for API Gateway to monitor HTTP Bad Gateway errors. Configure the metric filter to invoke a new Lambda function that stops the current deployment and starts the most recent successful deployment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
A company recently deployed its web application on AWS. The company is preparing for a large-scale sales event and must ensure that the web application can scale to meet the demand.The application's frontend infrastructure includes an Amazon CloudFront distribution that has an Amazon S3 bucket as an origin. The backend infrastructure includes an Amazon API Gateway API, several AWS Lambda functions, and an Amazon Aurora DB cluster.The company's DevOps engineer conducts a load test and identifies that the Lambda functions can fulfil the peak number of requests. However, the DevOps engineer notices request latency during the initial burst of requests. Most of the requests to the Lambda functions produce queries to the database. A large portion of the invocation time is used to establish database connections.Which combination

of steps will provide the application with the required scalability? (Choose three.)

A. Configure a higher reserved concurrency for the Lambda functions.
B. Configure a higher provisioned concurrency for the Lambda functions.
C. Convert the DB cluster to an Aurora global database. Add additional Aurora Replicas in AWS Regions based on the locations of the company's customers.
D. Refactor the Lambda functions. Move the code blocks that initialize database connections into the function handlers.
E. Use Amazon RDS Proxy to create a proxy for the Aurora database. Update the Lambda functions to use the proxy endpoints for database connections.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A company runs a web application that extends across multiple Availability Zones. The company uses an Application Load Balancer (ALB) for routing, AWS Fargate for the application, and Amazon Aurora for the application data. The company uses AWS CloudFormation templates to deploy the application. The company stores all Docker images in an Amazon Elastic Container Registry (Amazon ECR) repository in the same AWS account and AWS Region.A DevOps engineer needs to establish a disaster recovery (DR) process in another Region. The solution must meet an RPO of 8 hours and an RTO of 2 hours. The company sometimes needs more than 2 hours to build the Docker images from the Dockerfile.Which solution will meet the RTO and RPO requirements MOST cost-effectively?

A. Copy the CloudFormation templates and the Dockerfile to an Amazon S3 bucket in the DR Region. Use AWS Backup to configure automated Aurora cross-Region hourly snapshots. In case of DR, build the most recent Docker image and upload the Docker image to an ECR repository in the DR Region. Use the CloudFormation template that has the most recent Aurora snapshot and the Docker image from the ECR repository to launch a new CloudFormation stack in the DR Region. Update the application DNS records to point to the new AL
B.
C. Copy the CloudFormation templates to an Amazon S3 bucket in the DR Region. Use Amazon EventBridge to schedule an AWS Lambda function to take an hourly snapshot of the Aurora database and of the most recent Docker image in the ECR repository. Copy the snapshot and the Docker image to the DR Region. In case of DR, use the CloudFormation template with the most recent Aurora snapshot and the Docker image from the local ECR repository to launch a new CloudFormation stack in the DR Region.
D. Copy the CloudFormation templates to an Amazon S3 bucket in the DR Region. Deploy a second application CloudFormation stack in the DR Region. Reconfigure Aurora to be a global database. Update both CloudFormation stacks when a new application release in the current Region is needed. In case of DR, update the application DNS records to point to the new AL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A company's application runs on Amazon EC2 instances. The application writes to a log file that records the username, date, time, and source IP address of the login. The log is published to a log group in Amazon CloudWatch Logs.The company is performing a root cause analysis for an event that occurred on the previous day. The company needs to know the number of logins for a specific user from the past 7 days.Which solution

will provide this information?

A. Create a CloudWatch Logs metric filter on the log group. Use a filter pattern that matches the username. Publish a CloudWatch metric that sums the number of logins over the past 7 days.
B. Create a CloudWatch Logs subscription on the log group. Use a filter pattern that matches the username. Publish a CloudWatch metric that sums the number of logins over the past 7 days.
C. Create a CloudWatch Logs Insights query that uses an aggregation function to count the number of logins for the username over the past 7 days. Run the query against the log group.
D. Create a CloudWatch dashboard. Add a number widget that has a filter pattern that counts the number of logins for the username over the past 7 days directly from the log group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A company has an AWS CodeDeploy application. The application has a deployment group that uses a single tag group to identify instances for the deployment of Application. The single tag group configuration identifies instances that have Environment=Production and Name=ApplicationA tags for the deployment of ApplicationA.The company launches an additional Amazon EC2 instance with Department=Marketing, Environment=Production, and Name=ApplicationB tags. On the next CodeDeploy deployment of Application, the additional instance has ApplicationA installed on it. A DevOps engineer needs to configure the existing deployment group to prevent ApplicationA from being installed on the additional instance.Which solution will meet these requirements?

A. Change the current single tag group to include only the Environment=Production tag. Add another single tag group that includes only the Name=ApplicationA tag.
B. Change the current single tag group to include the Department=Marketing, Environment=production, and Name=ApplicationA tags.
C. Add another single tag group that includes only the Department=Marketing tag. Keep the Environment=Production and Name=ApplicationA tags with the current single tag group.
D. Change the current single tag group to include only the Environment=Production tag. Add another single tag group that includes only the Department=Marketing tag.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A company is launching an application that stores raw data in an Amazon S3 bucket. Three applications need to access the data to generate reports. The data must be redacted differently for each application before the applications can access the data.Which solution will meet these requirements?

A. Create an S3 bucket for each application. Configure S3 Same-Region Replication (SRR) from the raw data's S3 bucket to each application's S3 bucket. Configure each application to consume data from its own S3 bucket.
B. Create an Amazon Kinesis data stream. Create an AWS Lambda function that is invoked by object creation events in the raw dataâ€™s S3 bucket. Program the Lambda function to redact data for each application. Publish the data on the Kinesis data stream. Configure each application to consume data from the Kinesis data stream.
C. For each application, create an S3 access point that uses the raw data's S3 bucket as the destination.

Create an AWS Lambda function that is invoked by object creation events in the raw data's S3 bucket. Program the Lambda function to redact data for each application. Store the data in each application's S3 access point. Configure each application to consume data from its own S3 access point.

D. Create an S3 access point that uses the raw dataâ€™s S3 bucket as the destination. For each application, create an S3 Object Lambda access point that uses the S3 access point. Configure the AWS Lambda function for each S3 Object Lambda access point to redact data when objects are retrieved. Configure each application to consume data from its own S3 Object Lambda access point

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
A company uses AWS Control Tower and AWS CloudFormation to manage its AWS accounts and to create AWS resources. The company requires all Amazon S3 buckets to be encrypted with AWS Key Management Service (AWS KMS) when the S3 buckets are created in a CloudFormation stack.Which solution will meet this requirement?

A. Use AWS Organizations. Attach an SCP that denies the s3:PutObject permission if the request does not include an x-amz-server-side-encryption header that requests server-side encryption with AWS KMS keys (SSE-KMS).
B. Use AWS Control Tower with a multi-account environment. Configure and enable proactive AWS Control Tower controls on all OUs with CloudFormation hooks.
C. Use AWS Control Tower with a multi-account environment. Configure and enable detective AWS Control Tower controls on all OUs with CloudFormation hooks.
D. Use AWS Organizations. Create an AWS Config organizational rule to check whether a KMS encryption key is enabled for all S3 buckets. Deploy the rule. Create and apply an SCP to prevent users from stopping and deleting AWS Config across all AWS accounts,

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
A DevOps engineer has developed an AWS Lambda function. The Lambda function starts an AWS CloudFormation drift detection operation on all supported resources for a specific CloudFormation stack. The Lambda function then exits its invocation.The DevOps engineer has created an Amazon EventBridge scheduled rule that invokes the Lambda function every hour. An Amazon Simple Notification Service (Amazon SNS) topic already exists in the AWS account. The DevOps engineer has subscribed to the SNS topic to receive notifications.The DevOps engineer needs to receive a notification as soon as possible when drift is detected in this specific stack configuration.Which solution will meet these requirements?

A. Configure the existing EventBridge rule to also target the SNS topic. Configure an SNS subscription filter policy to match the CloudFormation stack. Attach the subscription filter policy to the SNS topic.
B. Create a second Lambda function to query the CloudFormation API for the drift detection results for the stack. Configure the second Lambda function to publish a message to the SNS topic if drift is detected. Adjust the existing EventBridge rule to also target the second Lambda function.
C. Configure Amazon GuardDuty in the account with drift detection for all CloudFormation stacks. Create a second EventBridge rule that reacts to the GuardDuty drift detection event finding for the specific CloudFormation stack. Configure the SNS topic as a target of the second EventBridge rule.
D. Configure AWS Config in the account. Use the cloudformation-stack-drift-detection-check managed rule.

Create a second EventBridge rule that reacts to a compliance change event for the CloudFormation stack. Configure the SNS topic as a target of the second EventBridge rule.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A company has deployed a complex container-based workload on AWS. The workload uses Amazon Managed Service for Prometheus for monitoring. The workload runs in an AmazonElastic Kubernetes Service (Amazon EKS) cluster in an AWS account.The companyâ€™s DevOps team wants to receive workload alerts by using the companyâ€™s Amazon Simple Notification Service (Amazon SNS) topic. The SNS topic is in the same AWS account as the EKS cluster.Which combination of steps will meet these requirements? (Choose three.)

A. Use the Amazon Managed Service for Prometheus remote write URL to send alerts to the SNS topic
B. Create an alerting rule that checks the availability of each of the workloadâ€™s containers.
C. Create an alert manager configuration for the SNS topic.
D. Modify the access policy of the SNS topic. Grant the aps.amazonaws.com service principal the sns:Publish permission and the sns:GetTopicAttributes permission for the SNS topic.
E. Modify the IAM role that Amazon Managed Service for Prometheus uses. Grant the role the sns:Publish permission and the sns:GetTopicAttributes permission for the SNS topic.
F. Create an OpenID Connect (OIDC) provider for the EKS cluster. Create a cluster service account. Grant the account the sns:Publish permission and the sns:GetTopicAttributes permission by using an IAM role.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
A company's organization in AWS Organizations has a single OU. The company runs Amazon EC2 instances in the OU accounts. The company needs to limit the use of each EC2 instanceâ€™s credentials to the specific EC2 instance that the credential is assigned to. A DevOps engineer must configure security for the EC2 instances.Which solution will meet these requirements?

A. Create an SCP that specifies the VPC CIDR block. Configure the SCP to check whether the value of the aws:VpcSourceIp condition key is in the specified block. In the same SCP check, check whether the values of the aws:EC2InstanceSourcePrivateIPv4 and aws:SourceVpc condition keys are the same. Deny access if either condition is false. Apply the SCP to the O
B. Create an SCP that checks whether the values of the aws:EC2InstanceSourceVPC and aws:SourceVpc condition keys are the same. Deny access if the values are not the same. In the same SCP check, check whether the values of the aws:EC2InstanceSourcePrivateIPv4 and aws:VpcSourceIp condition keys are the same. Deny access if the values are not the same. Apply the SCP to the O
C. Create an SCP that includes a list of acceptable VPC values and checks whether the value of the aws:SourceVpc condition key is in the list. In the same SCP check, define a list of acceptable IP address values and check whether the value of the aws:VpcSourceIp condition key is in the list. Deny access if either condition is false. Apply the SCP to each account in the organization.
D. Create an SCP that checks whether the values of the aws:EC2InstanceSourceVPC and aws:VpcSourceIp condition keys are the same. Deny access if the values are not the same. In the same SCP check, check whether the values of the aws:EC2InstanceSourcePrivateIPv4 and aws:SourceVpc condition keys are the same. Deny access if the values are not the same. Apply the SCP to each account in the organization.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A company has containerized all of its in-house quality control applications. The company is running Jenkins on Amazon EC2 instances, which require patching and upgrading. The compliance officer has requested a DevOps engineer begin encrypting build artifacts since they contain company intellectual property.What should the DevOps engineer do to accomplish this in the MOST maintainable manner?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A company has a fleet of Amazon EC2 instances that run Linux in a single AWS account. The company is using an AWS Systems Manager Automation task across the EC2 instances.During the most recent patch cycle, several EC2 instances went into an error state because of insufficient available disk space. A DevOps engineer needs to ensure that the EC2 instances have sufficient available disk space during the patching process in the future.Which combination of steps will meet these requirements? (Choose two.)

A. Ensure that the Amazon CloudWatch agent is installed on all EC2 instances.
B. Create a cron job that is installed on each EC2 instance to periodically delete temporary files.
C. Create an Amazon CloudWatch log group for the EC2 instances. Configure a cron job that is installed on each EC2 instance to write the available disk space to a CloudWatch log stream for the relevant EC2 instance.
D. Create an Amazon CloudWatch alarm to monitor available disk space on all EC2 instances. Add the alarm as a safety control to the Systems Manager Automation task.
E. Create an AWS Lambda function to periodically check for sufficient available disk space on all EC2 instances by evaluating each EC2 instance's respective Amazon CloudWatch log stream.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
A DevOps engineer is building an application that uses an AWS Lambda function to query an Amazon Aurora MySQL DB cluster. The Lambda function performs only read queries. Amazon EventBridge events invoke the Lambda function.As more events invoke the Lambda function each second, the database's latency increases and the database's throughput decreases. The DevOps engineer needs to improve the performance of the application.Which combination of steps will meet these requirements? (Choose three.)

A. Use Amazon RDS Proxy to create a proxy. Connect the proxy to the Aurora cluster reader endpoint. Set a maximum connections percentage on the proxy.
B. Implement database connection pooling inside the Lambda code. Set a maximum number of connections on the database connection pool.
C. Implement the database connection opening outside the Lambda event handler code.
D. Implement the database connection opening and closing inside the Lambda event handler code.
E. Connect to the proxy endpoint from the Lambda function.
F. Connect to the Aurora cluster endpoint from the Lambda function.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A company has an AWS CloudFormation stack that is deployed in a single AWS account. The company has configured the stack to send event notifications to an Amazon Simple Notification Service (Amazon SNS) topic.A DevOps engineer must implement an automated solution that applies a tag to the specific CloudFormation stack instance only after a successful stack update occurs. The DevOps engineer has created an AWS Lambda function that applies and updates this tag for the specific stack instance.Which solution will meet these requirements?

A. Run the AWS-UpdateCloudFormationStack AWS Systems ManagerAutomation runbook when Systems Manager detects an UPDATE_COMPLETE event for the instance status of the CloudFormation stack. Configure the runbook to invoke the Lambda function.
B. Create a custom AWS Config rule that produces a compliance change event if the CloudFormation stack has an UPDATE_COMPLETE instance status. Configure AWS Config to directly invoke the Lambda function to automatically remediate the change event.
C. Create an Amazon EventBridge rule that matches the UPDATE_COMPLETE event pattern for the instance status of the CloudFormation stack. Configure the rule to invoke the Lambda function.
D. Adjust the configuration of the CloudFormation stack to send notifications for only an UPDATE_COMPLETE instance status event to the SNS topic. Subscribe the Lambda function to the SNS topic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A company deploys an application to two AWS Regions. The application creates and stores objects in an Amazon S3 bucket that is in the same Region as the application. Both deployments of the application need to have access to all the objects and their metadata from both Regions. The company has configured two-way replication between the S3 buckets and has enabled S3 Replication metrics on each S3 bucket.A DevOps engineer needs to implement a solution that retries the replication process if an object fails to replicate.Which solution will meet these requirements?

A. Create an Amazon EventBridge rule that listens to S3 event notifications for failed replication events. Create an AWS Lambda function that downloads the failed replication object and then runs a PutObject command for the object to the destination bucket. Configure the EventBridge rule to invoke the Lambda function to handle the object that failed to replicate.

B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure S3 event notifications to send failed replication notifications to the SQS queue. Create an AWS Lambda function that downloads the failed replication object and then runs a PutObject command for the object to the destination bucket. Configure the Lambda function to poll the queue for notifications to process.
C. Create an Amazon EventBridge rule that listens to S3 event notifications for failed replications. Create an AWS Lambda function that downloads the failed replication object and then runs a PutObject command for the object to the destination bucket.
D. Create an AWS Lambda function that will use S3 batch operations to retry the replication on the existing object for a failed replication. Configure S3 event notifications to send failed replication notifications to the Lambda function.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A company needs to implement failover for its application. The application includes an Amazon CloudFront distribution and a public Application Load Balancer (ALB) in an AWS Region. The company has configured the ALB as the default origin for the distribution.After some recent application outages, the company wants a zero-second RTO. The company deploys the application to a secondary Region in a warm standby configuration. A DevOps engineer needs to automate the failover of the application to the secondary Region so that HTTP GET requests meet the desired RTO.Which solution will meet these requirements?

A. Create a second CloudFront distribution that has the secondary ALB as the default origin. Create Amazon Route 53 alias records that have a failover policy and Evaluate Target Health set to Yes for both CloudFront distributions. Update the application to use the new record set.
B. Create a new origin on the distribution for the secondary ALCreate a new origin group. Set the original ALB as the primary origin. Configure the origin group to fail over for HTTP 5xx status codes. Update the default behavior to use the origin group.
C. Create Amazon Route 53 alias records that have a failover policy and Evaluate Target Health set to Yes for both ALBs. Set the TTL of both records to 0. Update the distribution's origin to use the new record set.
D. Create a CloudFront function that detects HTTP 5xx status codes. Configure the function to return a 307 Temporary Redirect error response to the secondary ALB if the function detects 5xx status codes. Update the distribution's default behavior to send origin responses to the function.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A cloud team uses AWS Organizations and AWS IAM Identity Center (AWS Single Sign-On) to manage a company's AWS accounts. The company recently established a research team. The research team requires the ability to fully manage the resources in its account. The research team must not be able to create IAM users.The cloud team creates a Research Administrator permission set in IAM Identity Center for the research team. The permission set has the AdministratorAccess AWS managed policy attached. The cloud team must ensure that no one on the research team can create IAM users.Which solution will meet these requirements?

A. Create an IAM policy that denies the iam:CreateUser action. Attach the IAM policy to the Research Administrator permission set.
B. Create an IAM policy that allows all actions except the iam:CreateUser action. Use the IAM policy to set the permissions boundary for the Research Administrator permission set.

C. Create an SCP that denies the iam:CreateUser action. Attach the SCP to the research team's AWS account.
D. Create an AWS Lambda function that deletes IAM users. Create an Amazon EventBridge rule that detects the IAM CreateUser event. Configure the rule to invoke the Lambda function.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
A company releases a new application in a new AWS account. The application includes an AWS Lambda function that processes messages from an Amazon Simple Queue Service (Amazon SQS) standard queue. The Lambda function stores the results in an Amazon S3 bucket for further downstream processing. The Lambda function needs to process the messages within a specific period of time after the messages are published. The Lambda function has a batch size of 10 messages and takes a few seconds to process a batch of messages.As load increases on the application's first day of service, messages in the queue accumulate at a greater rate than the Lambda function can process the messages. Some messages miss the required processing timelines. The logs show that many messages in the queue have data that is not valid. The company needs to meet the timeline requirements for messages that have valid data.Which solution will meet these requirements?

A. Increase the Lambda function's batch size. Change the SQS standard queue to an SQS FIFO queue. Request a Lambda concurrency increase in the AWS Region.
B. Reduce the Lambda function's batch size. Increase the SQS message throughput quota. Request a Lambda concurrency increase in the AWS Region.
C. Increase the Lambda function's batch size. Configure S3 Transfer Acceleration on the S3 bucket. Configure an SQS dead-letter queue.
D. Keep the Lambda function's batch size the same. Configure the Lambda function to report failed batch items. Configure an SQS dead-letter queue.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A company has an application that runs on AWS Lambda and sends logs to Amazon CloudWatch Logs. An Amazon Kinesis data stream is subscribed to the log groups in CloudWatch Logs. A single consumer Lambda function processes the logs from the data stream and stores the logs in an Amazon S3 bucket.The companyâ €™s DevOps team has noticed high latency during the processing and ingestion of some logs.Which combination of steps will reduce the latency? (Choose three.)

A. Create a data stream consumer with enhanced fan-out. Set the Lambda function that processes the logs as the consumer.
B. Increase the ParallelizationFactor setting in the Lambda event source mapping.
C. Configure reserved concurrency for the Lambda function that processes the logs.
D. Increase the batch size in the Kinesis data stream.
E. Turn off the ReportBatchItemFailures setting in the Lambda event source mapping.
F. Increase the number of shards in the Kinesis data stream.

Correct Answer: ABF

Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A company operates sensitive workloads across the AWS accounts that are in the company's organization in AWS Organizations. The company uses an IP address range to delegate IP addresses for Amazon VPC CIDR blocks and all non-cloud hardware.The company needs a solution that prevents principals that are outside the companyâ€™s IP address range from performing AWS actions in the organization's accounts.Which solution will meet these requirements?

A. Configure AWS Firewall Manager for the organization. Create an AWS Network Firewall policy that allows only source traffic from the company's IP address range. Set the policy scope to all accounts in the organization.
B. In Organizations, create an SCP that denies source IP addresses that are outside of the companyâ€™s IP address range. Attach the SCP to the organization's root.
C. Configure Amazon GuardDuty for the organization. Create a GuardDuty trusted IP address list for the company's IP range. Activate the trusted IP list for the organization.
D. In Organizations, create an SCP that allows source IP addresses that are inside of the companyâ€™s IP address range. Attach the SCP to the organization's root.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A company deploys an application in two AWS Regions. The application currently uses an Amazon S3 bucket in the primary Region to store data.A DevOps engineer needs to ensure that the application is highly available in both Regions. The DevOps engineer has created a new S3 bucket in the secondary Region. All existing and new objects must be in both S3 buckets. The application must fail over between the Regions with no data loss.Which combination of steps will meet these requirements with the MOST operational efficiency? (Choose three.)

A. Create a new IAM role that allows the Amazon S3 and S3 Batch Operations service principals to assume the role that has the necessary permissions for S3 replication.
B. Create a new IAM role that allows the AWS Batch service principal to assume the role that has the necessary permissions for S3 replication.
C. Create an S3 Cross-Region Replication (CRR) rule on the source S3 bucket. Configure the rule to use the IAM role for Amazon S3 to replicate to the target S3 bucket.
D. Create a two-way replication rule on the source S3 bucket. Configure the rule to use the IAM role for Amazon S3 to replicate to the target S3 bucket.
E. Create an AWS Batch job that has an AWS Fargate orchestration type. Configure the job to use the IAM role for AWS Batch. Specify a Bash command to use the AWS CLI to synchronize the contents of the source S3 bucket and the target S3 bucket
F. Create an operation in S3 Batch Operations to replicate the contents of the source S3 bucket to the target S3 bucket. Configure the operation to use the IAM role for Amazon S3.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
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 a DelelionPolicy 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 with an AWS Lambda function with the DependsOn attribute specifying the S3 bucket, and an IAM role. Write the Lambda function to delete all objects from the bucket when RequestType is Delete.
C. Identify the resource that was not deleted. Manually empty the S3 bucket and then delete it.
D. Replace the EC2 and S3 bucket resources with a single AWS OpsWorks Stacks resource. Define a custom recipe for the stack to create and delete the EC2 instance and the S3 bucket.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company needs an automated process across all AWS accounts to isolate any compromised Amazon EC2 instances when the instances receive a specific tag.Which combination of steps will meet these requirements? (Choose two.)

A. Use AWS CloudFormation StackSets to deploy the CloudFormation stacks in all AWS accounts.
B. Create an SCP that has a Deny statement for the ec2:* action with a condition of "aws:RequestTag/ isolation": false.
C. Attach the SCP to the root of the organization.
D. Create an AWS CloudFormation template that creates an EC2 instance role that has no IAM policies attached. Configure the template to have a security group that has an explicit Deny rule on all traffic. Use the CloudFormation template to create an AWS Lambda function that attaches the IAM role to instances. Configure the Lambda function to add a network AC
E. Create an AWS CloudFormation template that creates an EC2 instance role that has no IAM policies attached. Configure the template to have a security group that has no inbound rules or outbound rules. Use the CloudFormation template to create an AWS Lambda function that attaches the IAM role to instances. Configure the Lambda function to replace any existing security groups with the new security group. Set up an Amazon EventBridge rule to invoke the Lambda function when a specific tag is applied to a compromised EC2 instance.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
A company manages multiple AWS accounts by using AWS Organizations with OUs for the different business

divisions. The company is updating their corporate network to use new IP address ranges. The company has 10 Amazon S3 buckets in different AWS accounts. The S3 buckets store reports for the different divisions. The S3 bucket configurations allow only private corporate network IP addresses to access the S3 buckets.A DevOps engineer needs to change the range of IP addresses that have permission to access the contents of the S3 buckets. The DevOps engineer also needs to revoke the permissions of two OUs in the company.Which solution will meet these requirements?

A. Create a new SCP that has two statements, one that allows access to the new range of IP addresses for all the S3 buckets and one that denies access to the old range of IP addresses for all the S3 buckets. Set a permissions boundary for the OrganizationAccountAccessRole role in the two OUs to deny access to the S3 buckets.
B. Create a new SCP that has a statement that allows only the new range of IP addresses to access the S3 buckets. Create another SCP that denies access to the S3 buckets. Attach the second SCP to the two OUs.
C. On all the S3 buckets, configure resource-based policies that allow only the new range of IP addresses to access the S3 buckets. Create a new SCP that denies access to the S3 buckets. Attach the SCP to the two OUs.
D. On all the S3 buckets, configure resource-based policies that allow only the new range of IP addresses to access the S3 buckets. Set a permissions boundary for the OrganizationAccountAccessRole role in the two OUs to deny access to the S3 buckets.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A company has started using AWS across several teams. Each team has multiple accounts and unique security profiles. The company manages the accounts in an organization in AWS Organizations. Each account has its own configuration and security controls.The company's DevOps team wants to use preventive and detective controls to govern all accounts. The DevOps team needs to ensure the security of accounts now and in the future as the company creates new accounts in the organization.Which solution will meet these requirements?

A. Use Organizations to create OUs that have appropriate SCPs attached for each team. Place team accounts in the appropriate OUs to apply security controls. Create any new team accounts in the appropriate OUs.
B. Create an AWS Control Tower landing zone. Configure OUs and appropriate controls in AWS Control Tower for the existing teams. Configure trusted access for AWS Control Tower. Enroll the existing accounts in the appropriate OUs that match the appropriate security policies for each team. Use AWS Control Tower to provision any new accounts.
C. Create AWS CloudFormation stack sets in the organization's management account. Configure a stack set that deploys AWS Config with configuration rules and remediation actions for all controls to each account in the organization. Update the stack sets to deploy to new accounts as the accounts are created.
D. Configure AWS Config to manage the AWS Config rules across all AWS accounts in the organization. Deploy conformance packs that provide AWS Config rules and remediation actions across the organization.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A company uses an AWS CodeCommit repository to store its source code and corresponding unit tests. The

company has configured an AWS CodePipeline pipeline that includes an AWS CodeBuild project that runs when code is merged to the main branch of the repository.The company wants the CodeBuild project to run the unit tests. If the unit tests pass, the CodeBuild project must tag the most recent commit.How should the company configure the CodeBuild project to meet these requirements?

A. Configure the CodeBuild project to use native Git to done the CodeCommit repository. Configure the project to run the unit tests. Configure the project to use native Git to create a tag and to push the Git tag to the repository if the code passes the unit tests.
B. Configure the CodeBuild projed to use native Git to done the CodeCommit repository. Configure the project to run the unit tests. Configure the project to use AWS CLI commands to create a new repository tag in the repository if the code passes the unit tests.
C. Configure the CodeBuild project to use AWS CLI commands to copy the code from the CodeCommit repository. Configure the project to run the unit tests. Configure the project to use AWS CLI commands to create a new Git tag in the repository if the code passes the unit tests.
D. Configure the CodeBuild project to use AWS CLI commands to copy the code from the CodeCommit repository. Configure the project to run the unit tests. Configure the project to use AWS CLI commands to create a new repository tag in the repository if the code passes the unit tests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A DevOps engineer manages a company's Amazon Elastic Container Service (Amazon ECS) cluster. The cluster runs on several Amazon EC2 instances that are in an Auto Scaling group. The DevOps engineer must implement a solution that logs and reviews all stopped tasks for errors.Which solution will meet these requirements?

A. Create an Amazon EventBridge rule to capture task state changes. Send the event to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to investigate stopped tasks.
B. Configure tasks to write log data in the embedded metric format. Store the logs in Amazon CloudWatch Logs. Monitor the ContainerInstanceCount metric for changes.
C. Configure the EC2 instances to store logs in Amazon CloudWatch Logs. Create a CloudWatch Contributor Insights rule that uses the EC2 instance log data. Use the Contributor Insights rule to investigate stopped tasks.
D. Configure an EC2 Auto Scaling lifecycle hook for the EC2_INSTANCE_TERMINATING scale-in event. Write the SystemEventLog file to Amazon S3. Use Amazon Athena to query the log file for errors.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
A company wants to deploy a workload on several hundred Amazon EC2 instances. The company will provision the EC2 instances in an Auto Scaling group by using a launch template.The workload will pull files from an Amazon S3 bucket, process the data, and put the results into a different S3 bucket. The EC2 instances must have least-privilege permissions and must use temporary security credentials.Which combination of steps will meet these requirements? (Choose two.)

A. Create an IAM role that has the appropriate permissions for S3 buckets Add the IAM role to an instance profile.

B. Update the launch template to include the IAM instance profile.
C. Create an IAM user that has the appropriate permissions for Amazon S3 Generate a secret key and token.
D. Create a trust anchor and profile Attach the IAM role to the profile.
E. Update the launch template Modify the user data to use the new secret key and token.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A company is using AWS CodeDeploy to automate software deployment. The deployment must meet these requirements:â€¢ 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. â€¢ A new fleet of instances must be launched for deploying a new revision automatically, with no manual provisioning.â€¢ 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.â€¢ Before routing traffic to the new fleet of instances, the temporary files generated during the deployment process must be deleted.â€¢ 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 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 BeforeBlockTraffic hook within appspec.yml to delete the temporary files.
C. Use an Application Load Balancer and a blue/green deployment. Associate the Auto Scaling group and the Application Load Balancer target group with the deployment group. Use the Automatically copy Auto Scaling group option, and use CodeDeployDefault.HalfAtAtime as the deployment configuration. Instruct AWS CodeDeploy to terminate the original instances in the deployment group, and use the BeforeAllowTraffic hook within appspec.yml to delete the temporary files.
D. Use an Application Load Balancer and an in-place deployment. Associate the Auto Scaling group and Application Load Balancer target group with the deployment group. Use the Automatically copy Auto Scaling group option, and use CodeDeployDefault.AllatOnce as a deployment configuration. Instruct AWS CodeDeploy to terminate the original instances in the deployment group, and use the BlockTraffic hook within appspec.yml to delete the temporary files.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
A company needs to adopt a multi-account strategy to deploy its applications and the associated CI/CD infrastructure. The company has created an organization in AWS Organizations that has all features enabled. The company has configured AWS Control Tower and has set up a landing zone.The company needs to use AWS Control Tower controls (guardrails) in all AWS accounts in the organization. The company must create the accounts for a multi-environment application and must ensure that all accounts are configured to an initial

baseline.Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Control Tower Account Factory Customization (AFC) blueprint that uses the baseline configuration. Use AWS Control Tower Account Factory to provision a dedicated AWS account for each environment and a CI/CD account by using the blueprint.
B. Use AWS Control Tower Account Factory to provision a dedicated AWS account for each environment and a CI/CD account. Use AWS CloudFormation StackSets to apply the baseline configuration to the new accounts.
C. Use Organizations to provision a multi-environment AWS account and a CI/CD account. In the Organizations management account, create an AWS Lambda function that assumes the Organizations access role to apply the baseline configuration to the new accounts.
D. Use Organizations to provision a dedicated AWS account for each environment, an audit account, and a CI/CD account. Use AWS CloudFormation StackSets to apply the baseline configuration to the new accounts.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
A DevOps team has created a Custom Lambda rule in AWS Config. The rule monitors Amazon Elastic Container Repository (Amazon ECR) policy statements for ecr:* actions. When a noncompliant repository is detected, Amazon EventBridge uses Amazon Simple Notification Service (Amazon SNS) to route the notification to a security team.When the custom AWS Config rule is evaluated, the AWS Lambda function fails to run.Which solution will resolve the issue?

A. Modify the Lambda function's resource policy to grant AWS Config permission to invoke the function.
B. Modify the SNS topic policy to include configuration changes for EventBridge to publish to the SNS topic.
C. Modify the Lambda function's execution role to include configuration changes for custom AWS Config rules.
D. Modify all the ECR repository policies to grant AWS Config access to the necessary ECR API actions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
A developer is creating a proof of concept for a new software as a service (SaaS) application. The application is in a shared development AWS account that is part of an organization in AWS Organizations.The developer needs to create service-linked IAM roles for the AWS services that are being considered for the proof of concept. The solution needs to give the developer the ability to create and configure the service-linked roles only.Which solution will meet these requirements?

A. Create an IAM user for the developer in the organization's management account. Configure a cross-account role in the development account for the developer to use. Limit the scope of the cross-account role to common services.
B. Add the developer to an IAM group. Attach the PowerUserAccess managed policy to the IAM group. Enforce multi-factor authentication (MFA) on the user account.
C. Add an SCP to the development account in Organizations. Configure the SCP with a Deny rule for iam:* to limit the developer's access.
D. Create an IAM role that has the necessary IAM access to allow the developer to create policies and roles.

Create and attach a permissions boundary to the role. Grant the developer access to assume the role.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
A company has an AWS CodePipeline pipeline that is configured with an Amazon S3 bucket in the eu-west-1 Region. The pipeline deploys an AWS Lambda application to the same Region. The pipeline consists of an AWS CodeBuild project build action and an AWS CloudFormation deploy action.The CodeBuild project uses the aws cloudformation package AWS CLI command to build an artifact that contains the Lambda function codeâ€™s .zip file and the CloudFormation template. The CloudFormation deploy action references the CloudFormation template from the output artifact of the CodeBuild projectâ€™s build action.The company wants to also deploy the Lambda application to the us-east-1 Region by using the pipeline in eu-west-1. A DevOps engineer has already updated the CodeBuild project to use the aws cloudformation package command to produce an additional output artifact for us-east-1.Which combination of additional steps should the DevOps engineer take to meet these requirements? (Choose two.)

A. Modify the CloudFormation template to include a parameter for the Lambda function codeâ€™s zip file location. Create a new CloudFormation deploy action for us-east-1 in the pipeline. Configure the new deploy action to pass in the us-east-1 artifact location as a parameter override.
B. Create a new CloudFormation deploy action for us-east-1 in the pipeline. Configure the new deploy action to use the CloudFormation template from the us-east-1 output artifact.
C. Create an S3 bucket in us-east-1. Configure the S3 bucket policy to allow CodePipeline to have read and write access.
D. Create an S3 bucket in us-east-1. Configure S3 Cross-Region Replication (CRR) from the S3 bucket in eu-west-1 to the S3 bucket in us-east-1.
E. Modify the pipeline to include the S3 bucket for us-east-1 as an artifact store. Create a new CloudFormation deploy action for us-east-1 in the pipeline. Configure the new deploy action to use the CloudFormation template from the us-east-1 output artifact.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A company uses AWS Organizations to manage its AWS accounts. The company wants its monitoring system to receive an alert when a root user logs in. The company also needs a dashboard to display any log activity that the root user generates.Which combination of steps will meet these requirements? (Choose three.)

A. Enable AWS Config with a multi-account aggregator. Configure log forwarding to Amazon CloudWatch Logs.
B. Create an Amazon QuickSight dashboard that uses an Amazon CloudWatch Logs query.
C. Create an Amazon CloudWatch Logs metric filter to match root user login events. Configure a CloudWatch alarm and an Amazon Simple Notification Service (Amazon SNS) topic to send alerts to the company's monitoring system.
D. Create an Amazon CloudWatch Logs subscription filter to match root user login events. Configure the filter to forward events to an Amazon Simple Notification Service (Amazon SNS) topic. Configure the SNS topic to send alerts to the company's monitoring system.
E. Create an AWS CloudTrail organization trail. Configure the organization trail to send events to Amazon CloudWatch Logs.

F. Create an Amazon CloudWatch dashboard that uses a CloudWatch Logs Insights query.

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A company uses AWS Organizations to manage its AWS accounts. A DevOps engineer must ensure that all users who access the AWS Management Console are authenticated through the companyâ€™s corporate identity provider (IdP).Which combination of steps will meet these requirements? (Choose two.)

A. Use Amazon GuardDuty with a delegated administrator account Use GuardDuty to enforce denial of IAM user logins.
B. Use AWS IAM Identity Center to configure identity federation with SAML 2.0.
C. Create a permissions boundary in AWS IAM Identity Center to deny password logins for IAM users.
D. Create IAM groups in the Organizations management account to apply consistent permissions for all IAM users.
E. Create an SCP in Organizations to deny password creation for IAM users.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A company has deployed a new platform that runs on Amazon Elastic Kubernetes Service (Amazon EKS). The new platform hosts web applications that users frequently update. The application developers build the Docker images for the applications and deploy the Docker images manually to the platform.The platform usage has increased to more than 500 users every day. Frequent updates, building the updated Docker images for the applications, and deploying the Docker images on the platform manually have all become difficult to manage.The company needs to receive an Amazon Simple Notification Service (Amazon SNS) notification if Docker image scanning returns any HIGH or CRITICAL findings for operating system or programming language package vulnerabilities.Which combination of steps will meet these requirements? (Choose two.)

A. Create an AWS CodeCommit repository to store the Dockerfile and Kubernetes deployment files. Create a pipeline in AWS CodePipeline. Use an Amazon S3 event to invoke the pipeline when a newer version of the Dockerfile is committed. Add a step to the pipeline to initiate the AWS CodeBuild project.
B. Create an AWS CodeCommit repository to store the Dockerfile and Kubernetes deployment files. Create a pipeline in AWS CodePipeline. Use an Amazon EventBridge event to invoke the pipeline when a newer version of the Dockerfile is committed. Add a step to the pipeline to initiate the AWS CodeBuild project.
C. Create an AWS CodeBuild project that builds the Docker images and stores the Docker images in an Amazon Elastic Container Registry (Amazon ECR) repository. Turn on basic scanning for the ECR repository. Create an Amazon EventBridge rule that monitors Amazon GuardDuty events. Configure the EventBridge rule to send an event to an SNS topic when the finding-severity-counts parameter is more than 0 at a CRITICAL or HIGH level.
D. Create an AWS CodeBuild project that builds the Docker images and stores the Docker images in an Amazon Elastic Container Registry (Amazon ECR) repository. Turn on enhanced scanning for the ECR repository. Create an Amazon EventBridge rule that monitors ECR image scan events. Configure the EventBridge rule to send an event to an SNS topic when the finding-severity-counts parameter is more than 0 at a CRITICAL or HIGH level.
E. Create an AWS CodeBuild project that scans the Dockerfile. Configure the project to build the Docker images and store the Docker images in an Amazon Elastic Container Registry (Amazon ECR) repository if

the scan is successful. Configure an SNS topic to provide notification if the scan returns any vulnerabilities.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
A company groups its AWS accounts in OUs in an organization in AWS Organizations. The company has deployed a set of Amazon API Gateway APIs in one of the Organizations accounts. The APIs are bound to the account's VPC and have no existing authentication mechanism. Only principals in a specific OU can have permissions to invoke the APIs.The company applies the following policy to the API Gateway interface VPC endpoint:The company also updates the API Gateway resource policies to deny invocations that do not come through the interface VPC endpoint. After the updates, the following error message appears during attempts to use the interface VPC endpoint URL to invoke an API: "User: anonymous is not authorized."Which combination of steps will solve this problem? (Choose two.)

A. Enable IAM authentication on all API methods by setting AWS JAM as the authorization method.
B. Create a token-based AWS Lambda authorizer that passes the caller's identity in a bearer token.
C. Create a request parameter-based AWS Lambda authorizer that passes the caller's identity in a combination of headers, query string parameters, stage variables, and $cortext variables.
D. Use Amazon Cognito user pools as the authorizer to control access to the AP
E. Verify the identity of the requester by using Signature Version 4 to sign client requests by using AWS credentials.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A company wants to decrease the time it takes to develop new features. The company uses AWS CodeBuild and AWS CodeDeploy to build and deploy its applications. The company uses AWS CodePipeline to deploy each microservice with its own CI/CD pipeline.The company needs more visibility into the average time between the release of new features and the average time to recover after a failed deployment.Which solution will provide this visibility with the LEAST configuration effort?

A. Program an AWS Lambda function that creates Amazon CloudWatch custom metrics with information about successful runs and failed runs for each pipeline. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. Use the metrics to build a CloudWatch dashboard.
B. Program an AWS Lambda function that creates Amazon CloudWatch custom metrics with information about successful runs and failed runs for each pipeline. Create an Amazon EventBridge rule to invoke the Lambda function after every successful run and after every failed run. Use the metrics to build a CloudWatch dashboard.
C. Program an AWS Lambda function that writes information about successful runs and failed runs to Amazon DynamoD
D. Program an AWS Lambda function that writes information about successful runs and failed runs to Amazon DynamoD

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A company uses Amazon EC2 as its primary compute platform. A DevOps team wants to audit the company's EC2 instances to check whether any prohibited applications have been installed on the EC2 instances.Which solution will meet these requirements with the MOST operational efficiency?

A. Configure AWS Systems Manager on each instance. Use AWS Systems Manager Inventory. Use Systems Manager resource data sync to synchronize and store findings in an Amazon S3 bucket. Create an AWS Lambda function that runs when new objects are added to the S3 bucket. Configure the Lambda function to identify prohibited applications.
B. Configure AWS Systems Manager on each instance. Use Systems Manager Inventory Create AWS Config rules that monitor changes from Systems Manager Inventory to identify prohibited applications.
C. Configure AWS Systems Manager on each instance. Use Systems Manager Inventory. Filter a trail in AWS CloudTrail for Systems Manager Inventory events to identify prohibited applications.
D. Designate Amazon CloudWatch Logs as the log destination for all application instances. Run an automated script across all instances to create an inventory of installed applications. Configure the script to forward the results to CloudWatch Logs. Create a CloudWatch alarm that uses filter patterns to search log data to identify prohibited applications.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A company has an event-driven JavaScript application. The application uses decoupled AWS managed services that publish, consume, and route events. During application testing, events are not delivered to the target that is specified by an Amazon EventBridge rule.A DevOps team must provide application testers with additional functionality to view, troubleshoot, and prevent the loss of events without redeployment of the

application.Which combination of steps should the DevOps team take to meet these requirements? (Choose three.)

A. Launch AWS Device Farm with a standard test environment and project to run a specific build of the application.
B. Create an Amazon S3 bucket. Enable AWS CloudTrail. Create a CloudTrail trail that specifies the S3 bucket as the storage location.
C. Configure the EventBridge rule to use an Amazon Simple Queue Service (Amazon SQS) standard queue as a dead-letter queue.
D. Configure the EventBridge rule to use an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a dead-letter queue.
E. Create a log group in Amazon CloudWatch Logs Specify the log group as an additional target of the EventBridge rule.
F. Update the application code base to use the AWS X-Ray SDK tracing feature to instrument the code with support for the X-Amzn-Trace-Id header.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
A company is migrating its container-based workloads to an AWS Organizations multi-account environment. The environment consists of application workload accounts that the company uses to deploy and run the containerized workloads. The company has also provisioned a shared services account for shared workloads in the organization.The company must follow strict compliance regulations. All container images must receive security scanning before they are deployed to any environment. Images can be consumed by downstream deployment mechanisms after the images pass a scan with no critical vulnerabilities. Pre-scan and post-scan images must be isolated from one another so that a deployment can never use pre-scan images.A DevOps engineer needs to create a strategy to centralize this process.Which combination of steps will meet these requirements with the LEAST administrative overhead? (Choose two.)

A. Create Amazon Elastic Container Registry (Amazon ECR) repositories in the shared services account: one repository for each pre-scan image and one repository for each post-scan image. Configure Amazon ECR image scanning to run on new image pushes to the pre-scan repositories. Use resource-based policies to grant the organization write access to the pre-scan repositories and read access to the post-scan repositories.
B. Create pre-scan Amazon Elastic Container Registry (Amazon ECR) repositories in each account that publishes container images. Create repositories for post-scan images in the shared services account. Configure Amazon ECR image scanning to run on new image pushes to the pre-scan repositories. Use resource-based policies to grant the organization read access to the post-scan repositories.
C. Configure image replication for each image from the image's pre-scan repository to the image's post-scan repository.
D. Create a pipeline in AWS CodePipeline for each pre-scan repository. Create a source stage that runs when new images are pushed to the pre-scan repositories. Create a stage that uses AWS CodeBuild as the action provider. Write a buildspec.yaml definition that determines the image scanning status and pushes images without critical vulnerabilities to the post-scan repositories.
E. Create an AWS Lambda function. Create an Amazon EventBridge rule that reacts to image scanning completed events and invokes the Lambda function. Write function code that determines the image scanning status and pushes images without critical vulnerabilities to the post-scan repositories.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A company uses an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to deploy its web applications on containers. The web applications contain confidential data that cannot be decrypted without specific credentials.A DevOps engineer has stored the credentials in AWS Secrets Manager. The secrets are encrypted by an AWS Key Management Service (AWS KMS) customer managed key. A Kubernetes service account for a third-party tool makes the secrets available to the applications. The service account assumes an IAM role that the company created to access the secrets.The service account receives an Access Denied (403 Forbidden) error while trying to retrieve the secrets from Secrets Manager.What is the root cause of this issue?

A. The IAM role that is attached to the EKS cluster does not have access to retrieve the secrets from Secrets Manager.
B. The key policy for the customer managed key does not allow the Kubernetes service account IAM role to use the key.
C. The key policy for the customer managed key does not allow the EKS cluster IAM role to use the key.
D. The IAM role that is assumed by the Kubernetes service account does not have permission to access the EKS cluster.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A company runs an application on one Amazon EC2 instance. Application metadata is stored in Amazon S3 and must be retrieved if the instance is restarted. The instance must restart or relaunch automatically if the instance becomes unresponsive.Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm for the StatusCheckFailed metric. Use the recover action to stop and start the instance. Use an S3 event notification to push the metadata to the instance when the instance is back up and running.
B. Configure AWS OpsWorks, and use the auto healing feature to stop and start the instance. Use a lifecycle event in OpsWorks to pull the metadata from Amazon S3 and update it on the instance.
C. Use EC2 Auto Recovery to automatically stop and start the instance in case of a failure. Use an S3 event notification to push the metadata to the instance when the instance is back up and running.
D. Use AWS CloudFormation to create an EC2 instance that includes the UserData property for the EC2 resource. Add a command in UserData to retrieve the application metadata from Amazon S3.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
A company is migrating its product development teams from an on-premises data center to a hybrid environment. The new environment will add four AWS Regions and will give the developers the ability to use the Region that is geographically closest to them.All the development teams use a shared set of Linux applications. The on-premises data center stores the applications on a NetApp ONTAP storage device. The storage volume is mounted read-only on the development on-premises VMs. The company updates the applications on the shared volume once a week.A DevOps engineer needs to replicate the data to all the new Regions. The DevOps engineer must ensure that the data is always up to date with deduplication. The data

also must not be dependent on the availability of the on-premises storage device.Which solution will meet these requirements?

A. Create an Amazon S3 File Gateway in the on-premises data center. Create S3 buckets in each Region. Set up a cron job to copy the data from the storage device to the S3 File Gateway. Set up S3 Cross-Region Replication (CRR) to the S3 buckets in each Region.
B. Create an Amazon FSx File Gateway in one Region. Create file servers in Amazon FSx for Windows File Server in each Region. Set up a cron job to copy the data from the storage device to the FSx File Gateway.
C. Create Multi-AZ Amazon FSx for NetApp ONTAP instances and volumes in each Region. Configure a scheduled SnapMirror relationship between the on-premises storage device and the FSx for ONTAP instances.
D. Create an Amazon Elastic File System (Amazon EFS) file system in each Region. Deploy an AWS DataSync agent in the on-premises data center. Configure a schedule for DataSync to copy the data to Amazon EFS daily.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A company has an application that stores data that includes personally identifiable information (PII) in an Amazon S3 bucket. All data is encrypted with AWS Key Management Service (AWS KMS) customer managed keys. All AWS resources are deployed from an AWS CloudFormation template.A DevOps engineer needs to set up a development environment for the application in a different AWS account. The data in the development environment's S3 bucket needs to be updated once a week from the production environment's S3 bucket.The company must not move PII from the production environment without anonymizing the PII first. The data in each environment must be encrypted with different KMS customer managed keys.Which combination of steps should the DevOps engineer take to meet these requirements? (Choose two.)

A. Activate Amazon Macie on the S3 bucket in the production account. Create an AWS Step Functions state machine to initiate a discovery job and redact all PII before copying files to the S3 bucket in the development account. Give the state machine tasks decrypt permissions on the KMS key in the production account. Give the state machine tasks encrypt permissions on the KMS key in the development account.
B. Set up S3 replication between the production S3 bucket and the development S3 bucket. Activate Amazon Macie on the development S3 bucket. Create an AWS Step Functions state machine to initiate a discovery job and redact all PII as the files are copied to the development S3 bucket. Give the state machine tasks encrypt and decrypt permissions on the KMS key in the development account.
C. Set up an S3 Batch Operations job to copy files from the production S3 bucket to the development S3 bucket. In the development account, configure an AWS Lambda function to redact ail PI
D. Create a development environment from the CloudFormation template in the development account. Schedule an Amazon EventBridge rule to start the AWS Step Functions state machine once a week.
E. Create a development environment from the CloudFormation template in the development account. Schedule a cron job on an Amazon EC2 instance to run once a week to start the S3 Batch Operations job.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
A company uses an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host its machine learning (ML) application. As the ML model and the container image size grow, the time that new pods take to start up

has increased to several minutes.A DevOps engineer needs to reduce the startup time to seconds. The solution must also reduce the startup time to seconds when the pod runs on nodes that were recently added to the cluster.The DevOps engineer creates an Amazon EventBridge rule that invokes an automation in AWS Systems Manager. The automation prefetches the container images from an Amazon Elastic Container Registry (Amazon ECR) repository when new images are pushed to the repository. The DevOps engineer also configures tags to be applied to the cluster and the node groups.What should the DevOps engineer do next to meet the requirements?

A. Create an IAM role that has a policy that allows EventBridge to use Systems Manager to run commands in the EKS cluster's control plane nodes. Create a Systems Manager State Manager association that uses the control plane nodes' tags to prefetch corresponding container images.
B. Create an IAM role that has a policy that allows EventBridge to use Systems Manager to run commands in the EKS cluster's nodes. Create a Systems Manager State Manager association that uses the nodes' machine size to prefetch corresponding container images.
C. Create an IAM role that has a policy that allows EventBridge to use Systems Manager to run commands in the EKS cluster's nodes. Create a Systems Manager State Manager association that uses the nodes' tags to prefetch corresponding container images.
D. Create an IAM role that has a policy that allows EventBridge to use Systems Manager to run commands in the EKS cluster's control plane nodes. Create a Systems Manager State Manager association that uses the nodes' tags to prefetch corresponding container images.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A company's application has an API that retrieves workload metrics. The company needs to audit, analyze, and visualize these metrics from the application to detect issues at scale.Which combination of steps will meet these requirements? (Choose three.)

A. Configure an Amazon EventBridge schedule to invoke an AWS Lambda function that calls the API to retrieve workload metrics. Store the workload metric data in an Amazon S3 bucket.
B. Configure an Amazon EventBridge schedule to invoke an AWS Lambda function that calls the API to retrieve workload metrics. Store the workload metric data in an Amazon DynamoDB table that has a DynamoDB stream enabled.
C. Create an AWS Glue crawler to catalog the workload metric data in the Amazon S3 bucket. Create views in Amazon Athena for the cataloged data.
D. Connect an AWS Glue crawler to the Amazon DynamoDB stream to catalog the workload metric data. Create views in Amazon Athena for the cataloged data.
E. Create Amazon QuickSight datasets from the Amazon Athena views. Create a QuickSight analysis to visualize the workload metric data as a dashboard.
F. Create an Amazon CloudWatch dashboard that has custom widgets that invoke AWS Lambda functions. Configure the Lambda functions to query the workload metrics data from the Amazon Athena views.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
A DevOps engineer is building the infrastructure for an application. The application needs to run on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that includes Amazon EC2 instances. The EC2 instances

need to use an Amazon Elastic File System (Amazon EFS) file system as a storage backend. The Amazon EFS Container Storage Interface (CSI) driver is installed on the EKS cluster.When the DevOps engineer starts the application, the EC2 instances do not mount the EFS file system.Which solutions will fix the problem? (Choose three.)

A. Switch the EKS nodes from Amazon EC2 to AWS Fargate.
B. Add an inbound rule to the EFS file systemâ€™s security group to allow NFS traffic from the EKS cluster.
C. Create an IAM role that allows the Amazon EFS CSI driver to interact with the file system
D. Set up AWS DataSync to configure file transfer between the EFS file system and the EKS nodes.
E. Create a mount target for the EFS file system in the subnet of the EKS nodes.
F. Disable encryption or the EFS file system.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
A company deploys an application on on-premises devices in the companyâ€™s on-premises data center. The company uses an AWS Direct Connect connection between the data center and the company's AWS account. During initial setup of the on-premises devices and during application updates, the application needs to retrieve configuration files from an Amazon Elastic File System (Amazon EFS) file system.All traffic from the on-premises devices to Amazon EFS must remain private and encrypted. The on-premises devices must follow the principle of least privilege for AWS access. The company's DevOps team needs the ability to revoke access from a single device without affecting the access of the other devices.Which combination of steps will meet these requirements? (Choose two.)

A. Create an IAM user that has an access key and a secret key for each device. Attach the AmazonElasticFileSystemFullAccess policy to all IAM users. Configure the AWS CLI on the on-premises devices to use the IAM user's access key and secret key.
B. Generate certificates for each on-premises device in AWS Private Certificate Authority. Create a trust anchor in IAM Roles Anywhere that references an AWS Private C
C. Create an IAM user that has an access key and a secret key for all devices. Attach the AmazonElasticFileSystemClientReadWriteAccess policy to the IAM user. Configure the AWS CLI on the on-premises devices to use the IAM user's access key and secret key.
D. Use the amazon-efs-utils package to mount the EFS file system.
E. Use the native Linux NFS client to mount the EFS file system.

Correct Answer: BAD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
A DevOps engineer is setting up an Amazon Elastic Container Service (Amazon ECS) blue/green deployment for an application by using AWS CodeDeploy and AWS CloudFormation. During the deployment window, the application must be highly available and CodeDeploy must shift 10% of traffic to a new version of the application every minute until all traffic is shifted.Which configuration should the DevOps engineer add in the CloudFormation template to meet these requirements?

A. Add an AppSpec file with the CodeDeployDefault.ECSLinearl OPercentEveryl Minutes deployment configuration.

B. Add the AWS::CodeDeployBlueGreen transform and the AWS::CodeDeploy::BlueGreen hook parameter with the CodeDeployDefault.ECSLinear10PercentEvery1Minutes deployment configuration.
C. Add an AppSpec file with the ECSCanary10Percent5Minutes deployment configuration.
D. Add the AWS::CodeDeployBlueGreen transform and the AWS::CodeDepioy::BlueGreen hook parameter with the ECSCanary10Percent5Minutes deployment configuration.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A company uses an organization in AWS Organizations to manage its AWS accounts. The company's DevOps team has developed an AWS Lambda function that calls the Organizations API to create new AWS accounts.The Lambda function runs in the organization's management account. The DevOps team needs to move the Lambda function from the management account to a dedicated AWS account. The DevOps team must ensure that the Lambda function has the ability to create new AWS accounts only in Organizations before the team deploys the Lambda function to the new account.Which solution will meet these requirements?

A. In the management account, create a new IAM role that has the necessary permission to create new accounts in Organizations. Allow the role to be assumed by the Lambda execution role in the new AWS account. Update the Lambda function code to assume the role when the Lambda function creates new AWS accounts. Update the Lambda execution role to ensure that it has permission to assume the new role.
B. In the management account, turn on delegated administration for Organizations. Create a new delegation policy that grants the new AWS account permission to create new AWS accounts in Organizations. Ensure that the Lambda execution role has the organizations:CreateAccount permission.
C. In the management account, create a new IAM role that has the necessary permission to create new accounts in Organizations. Allow the role to be assumed by the Lambda service principal. Update the Lambda function code to assume the role when the Lambda function creates new AWS accounts. Update the Lambda execution role to ensure that it has permission to assume the new role.
D. In the management account, enable AWS Control Tower. Turn on delegated administration for AWS Control Tower. Create a resource policy that allows the new AWS account to create new AWS accounts in AWS Control Tower. Update the Lambda function code to use the AWS Control Tower API in the new AWS account. Ensure that the Lambda execution role has the controltower:CreateManagedAccount permission.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
A company has deployed an application in a single AWS Region. The application backend uses Amazon DynamoDB tables and Amazon S3 buckets.The company wants to deploy the application in a secondary Region. The company must ensure that the data in the DynamoDB tables and the S3 buckets persists across both Regions. The data must also immediately propagate across Regions.Which solution will meet these requirements with the MOST operational efficiency?

A. Implement two-way S3 bucket replication between the primary Region's S3 buckets and the secondary Regionâ€™s S3 buckets. Convert the DynamoDB tables into global tables. Set the secondary Region as the additional Region.
B. Implement S3 Batch Operations copy jobs between the primary Region and the secondary Region for all S3 buckets. Convert the DynamoDB tables into global tables. Set the secondary Region as the additional

Region.

C. Implement two-way S3 bucket replication between the primary Region's S3 buckets and the secondary Region's S3 buckets. Enable DynamoDB streams on the DynamoDB tables in both Regions. In each Region, create an AWS Lambda function that subscribes to the DynamoDB streams. Configure the Lambda function to copy new records to the DynamoDB tables in the other Region.
D. Implement S3 Batch Operations copy jobs between the primary Region and the secondary Region for all S3 buckets. Enable DynamoDB streams on the DynamoDB tables in both Regions. In each Region, create an AWS Lambda function that subscribes to the DynamoDB streams. Configure the Lambda function to copy new records to the DynamoDB tables in the other Region.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A company has configured Amazon RDS storage autoscaling for its RDS DB instances. A DevOps team needs to visualize the autoscaling events on an Amazon CloudWatch dashboard.Which solution will meet this requirement?

A. Create an Amazon EventBridge rule that reacts to RDS storage autoscaling events from RDS events. Create an AWS Lambda function that publishes a CloudWatch custom metric. Configure the EventBridge rule to invoke the Lambda function. Visualize the custom metric by using the CloudWatch dashboard.
B. Create a trail by using AWS CloudTrail with management events configured. Configure the trail to send the management events to Amazon CloudWatch Logs. Create a metric filter in CloudWatch Logs to match the RDS storage autoscaling events. Visualize the metric filter by using the CloudWatch dashboard.
C. Create an Amazon EventBridge rule that reacts to RDS storage autoscaling events from the RDS events. Create a CloudWatch alarm. Configure the EventBridge rule to change the status of the CloudWatch alarm. Visualize the alarm status by using the CloudWatch dashboard.
D. Create a trail by using AWS CloudTrail with data events configured. Configure the trail to send the data events to Amazon CloudWatch Logs. Create a metric filter in CloudWatch Logs to match the RDS storage autoscaling events. Visualize the metric filter by using the CloudWatch dashboard.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A company has multiple AWS accounts. The company uses AWS IAM Identity Center (AWS Single Sign-On) that is integrated with AWS Toolkit for Microsoft Azure DevOps. The attributes for access control feature is enabled in IAM Identity Center.The attribute mapping list contains two entries. The department key is mapped to ${path:enterprise.department}. The costCenter key is mapped to ${path:enterprise.costCenter}.All existing Amazon EC2 instances have a department tag that corresponds to three company departments (d1, d2, d3). A DevOps engineer must create policies based on the matching attributes. The policies must minimize administrative effort and must grant each Azure AD user access to only the EC2 instances that are tagged with the userâ€™s respective department name.Which condition key should the DevOps engineer include in the custom permissions policies to meet these requirements?

A.
B.
C.
D.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
A company uses containers for its applications. The company learns that some container images are missing required security configurations.A DevOps engineer needs to implement a solution to create a standard base image. The solution must publish the base image weekly to the us-west-2 Region, us-east-2 Region, and eu-central-1 Region.Which solution will meet these requirements?

A. Create an EC2 Image Builder pipeline that uses a container recipe to build the image. Configure the pipeline to distribute the image to an Amazon Elastic Container Registry (Amazon ECR) repository in us-west-2. Configure ECR replication from us-west-2 to us-east-2 and from us-east-2 to eu-central-1. Configure the pipeline to run weekly.
B. Create an AWS CodePipeline pipeline that uses an AWS CodeBuild project to build the image. Use AWS CodeDeploy to publish the image to an Amazon Elastic Container Registry (Amazon ECR) repository in us-west-2. Configure ECR replication from us-west-2 to us-east-2 and from us-east-2 to eu-central-1. Configure the pipeline to run weekly.
C. Create an EC2 Image Builder pipeline that uses a container recipe to build the image. Configure the pipeline to distribute the image to Amazon Elastic Container Registry (Amazon ECR) repositories in all three Regions. Configure the pipeline to run weekly.
D. Create an AWS CodePipeline pipeline that uses an AWS CodeBuild project to build the image. Use AWS CodeDeploy to publish the image to Amazon Elastic Container Registry (Amazon ECR) repositories in all three Regions. Configure the pipeline to run weekly.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A DevOps engineer needs to implement a solution to install antivirus software on all the Amazon EC2 instances in an AWS account. The EC2 instances run the most recent version of Amazon Linux.The solution must detect all instances and must use an AWS Systems Manager document to install the software if the software is not present.Which solution will meet these requirements?

A. Create an association in Systems Manager State Manager. Target all the managed nodes. Include the software in the association. Configure the association to use the Systems Manager document.
B. Set up AWS Config to record all the resources in the account. Create an AWS Config custom rule to determine if the software is installed on all the EC2 instances. Configure an automatic remediation action that uses the Systems Manager document for noncompliant EC2 instances.
C. Activate Amazon EC2 scanning on Amazon Inspector to determine if the software is installed on all the EC2 instances. Associate the findings with the Systems Manager document.
D. Create an Amazon EventBridge rule that uses AWS CloudTrail to detect the Runinstances API call. Configure inventory collection in Systems Manager Inventory to determine if the software is installed on the EC2 instances. Associate the Systems Manager inventory with the Systems Manager document.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
A company needs to increase the security of the container images that run in its production environment. The company wants to integrate operating system scanning and programming language package vulnerability scanning for the containers in its CI/CD pipeline. The CI/CD pipeline is an AWS CodePipeline pipeline that includes an AWS CodeBuild build project, AWS CodeDeploy actions, and an Amazon Elastic Container Registry (Amazon ECR) repository.A DevOps engineer needs to add an image scan to the CI/CD pipeline. The CI/CD pipeline must deploy only images without CRITICAL and HIGH findings into production.Which combination of steps will meet these requirements? (Choose two.)

A. Use Amazon ECR basic scanning.
B. Use Amazon ECR enhanced scanning.
C. Configure Amazon ECR to submit a Rejected status to the CI/CD pipeline when the image scan returns CRITICAL or HIGH findings.
D. Configure an Amazon EventBridge rule to invoke an AWS Lambda function when the image scan is completed. Configure the Lambda function to consume the Amazon Inspector scan status and to submit an Approved or Rejected status to the CI/CD pipeline.
E. Configure an Amazon EventBridge rule to invoke an AWS Lambda function when the image scan is completed. Configure the Lambda function to consume the Clair scan status and to submit an Approved or Rejected status to the CI/CD pipeline.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A company's DevOps team manages a set of AWS accounts that are in an organization in AWS Organizations.The company needs a solution that ensures that all Amazon EC2 instances use approved AM Is that the DevOps team manages. The solution also must remediate the usage of AMIs that are not approved. The individual account administrators must not be able to remove the restriction to use approved AMIs.Which solution will meet these requirements?

A. Use AWS CloudFormation StackSets to deploy an Amazon EventBridge rule to each account. Configure the rule to react to AWS CloudTrail events for Amazon EC2 and to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the DevOps team to the SNS topic.
B. Use AWS CloudFormation StackSets to deploy the approved-amis-by-id AWS Config managed rule to each account. Configure the rule with the list of approved AMIs. Configure the rule to run the AWS-StopEC2Instance AWS Systems Manager Automation runbook for the noncompliant EC2 instances.
C. Create an AWS Lambda function that processes AWS CloudTrail events for Amazon EC2. Configure the Lambda function to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the DevOps team to the SNS topic. Deploy the Lambda function in each account in the organization. Create an Amazon EventBridge rule in each account. Configure the EventBridge rules to react to AWS CloudTrail events for Amazon EC2 and to invoke the Lambda function.
D. Enable AWS Config across the organization. Create a conformance pack that uses the approved-amis-by-id AWS Config managed rule with the list of approved AMIs. Deploy the conformance pack across the organization. Configure the rule to run the AWS-StopEC2Instance AWS Systems Manager Automation runbook for the noncompliant EC2 instances.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
A company gives its employees limited rights to AWS. DevOps engineers have the ability to assume an administrator role. For tracking purposes, the security team wants to receive a near-real-time notification when the administrator role is assumed.How should this be accomplished?

A. Configure AWS Config to publish logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and send a notification to the security team when the administrator role is assumed.
B. Configure Amazon GuardDuty to monitor when the administrator role is assumed and send a notification to the security team.
C. Create an Amazon EventBridge event rule using an AWS Management Console sign-in events event pattern that publishes a message to an Amazon SNS topic if the administrator role is assumed.
D. Create an Amazon EventBridge events rule using an AWS API call that uses an AWS CloudTrail event pattern to invoke an AWS Lambda function that publishes a message to an Amazon SNS topic if the administrator role is assumed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
A company needs a strategy for failover and disaster recovery of its data and application. The application uses a MySQL database and Amazon EC2 instances. The company requires a maximum RPO of 2 hours and a maximum RTO of 10 minutes for its data and application at all times.Which combination of deployment strategies will meet these requirements? (Choose two.)

A. Create an Amazon Aurora Single-AZ cluster in multiple AWS Regions as the data store. Use Aurora's automatic recovery capabilities in the event of a disaster.
B. Create an Amazon Aurora global database in two AWS Regions as the data store. In the event of a failure, promote the secondary Region to the primary for the application. Update the application to use the Aurora cluster endpoint in the secondary Region.
C. Create an Amazon Aurora cluster in multiple AWS Regions as the data store. Use a Network Load Balancer to balance the database traffic in different Regions.
D. Set up the application in two AWS Regions. Use Amazon Route 53 failover routing that points to Application Load Balancers in both Regions. Use health checks and Auto Scaling groups in each Region.
E. Set up the application in two AWS Regions. Configure AWS Global Accelerator to point to Application Load Balancers (ALBs) in both Regions. Add both ALBs to a single endpoint group. Use health checks and Auto Scaling groups in each Region.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A developer is using the AWS Serverless Application Model (AWS SAM) to create a prototype for an AWS Lambda function. The AWS SAM template contains an AWS::Serverless::Function resource that has the CodeUri property that points to an Amazon S3 location. The developer wants to identify the correct commands for deployment before creating a CI/CD pipeline.The developer creates an archive of the Lambda function code named package.zip. The developer uploads the .zip file archive to the S3 location specified in the CodeUri

property. The developer runs the sam deploy command and deploys the Lambda function. The developer updates the Lambda function code and uses the same steps to deploy the new version of the Lambda function. The sam deploy command fails and returns an error of no changes to deploy.Which solutions will deploy the new version? (Choose two.)

A. Use the aws cloudformation update-stack command instead of the sam deploy command.
B. Use the aws cloudformation update-stack-instances command instead of the sam deploy command.
C. Update the CodeUri property to reference the local application code folder. Use the sam deploy command.
D. Update the CodeUri property to reference the local application code folder. Use the aws cloudformation create-change-set command and the aws cloudformation execute-change-set command.
E. Update the CodeUri property to reference the local application code folder. Use the aws cloudformation package command and the aws cloudformation deploy command.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
A company runs its container workloads in AWS App Runner. A DevOps engineer manages the company's container repository in Amazon Elastic Container Registry (Amazon ECR).The DevOps engineer must implement a solution that continuously monitors the container repository. The solution must create a new container image when the solution detects an operating system vulnerability or language package vulnerability.Which solution will meet these requirements?

A. Use EC2 Image Builder to create a container image pipeline. Use Amazon ECR as the target repository. Turn on enhanced scanning on the ECR repository. Create an Amazon EventBridge rule to capture an Inspector? finding event. Use the event to invoke the image pipeline. Re-upload the container to the repository.
B. Use EC2 Image Builder to create a container image pipeline. Use Amazon ECR as the target repository. Enable Amazon GuardDuty Malware Protection on the container workload. Create an Amazon EventBridge rule to capture a GuardDuty finding event. Use the event to invoke the image pipeline.
C. Create an AWS CodeBuild project to create a container image. Use Amazon ECR as the target repository. Turn on basic scanning on the repository. Create an Amazon EventBridge rule to capture an ECR image action event. Use the event to invoke the CodeBuild project. Re-upload the container to the repository.
D. Create an AWS CodeBuild project to create a container image. Use Amazon ECR as the target repository. Configure AWS Systems Manager Compliance to scan all managed nodes. Create an Amazon EventBridge rule to capture a configuration compliance state change event. Use the event to invoke the CodeBuild project.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A company wants to use AWS Systems Manager documents to bootstrap physical laptops for developers. The bootstrap code is stored in GitHub. A DevOps engineer has already created a Systems Manager activation, installed the Systems Manager agent with the registration code, and installed an activation ID on all the laptops.Which set of steps should be taken next?

A. Configure the Systems Manager document to use the AWS-RunShellScript command to copy the files from GitHub to Amazon S3, then use the aws-downloadContent plugin with a sourceType of S3.

B. Configure the Systems Manager document to use the aws-configurePackage plugin with an install action and point to the Git repository.
C. Configure the Systems Manager document to use the aws-downloadContent plugin with a sourceType of GitHub and sourceInfo with the repository details.
D. Configure the Systems Manager document to use the aws:softwareInventory plugin and run the script from the Git repository.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A company's development team uses AWS CloudFormation to deploy its application resources. The team must use CloudFormation for all changes to the environment. The team cannot use the AWS Management Console or the AWS CLI to make manual changes directly.The team uses a developer IAM role to access the environment. The role is configured with the AdministratorAccess managed IAM policy. The company has created a new CloudFormationDeployment IAM role that has the following policy attached:The company wants to ensure that only CloudFormation can use the new role. The development team cannot make any manual changes to the deployed resources.Which combination of steps will meet these requirements? (Choose three.)

A. Remove the AdministratorAccess policy. Assign the ReadOnlyAccess managed IAM policy to the developer role. Instruct the developers to use the CloudFormationDeployment role as a CloudFormation service role when the developers deploy new stacks.
B. Update the trust policy of the CloudFormationDeployment role to allow the developer IAM role to assume the CloudFormationDeployment role.
C. Configure the developer IAM role to be able to get and pass the CloudFormationDeployment role if iam:PassedToService equals . Configure the CloudFormationDeployment role to allow all cloudformation actions for all resources.
D. Update the trust policy of the CloudFormationDeployment role to allow the cloudformation.amazonaws.com AWS principal to perform the iam:AssumeRole action.
E. Remove the AdministratorAccess policy. Assign the ReadOnlyAccess managed IAM policy to the developer role. Instruct the developers to assume the CloudFormationDeployment role when the developers deploy new stacks.
F. Add an IAM policy to the CloudFormationDeployment role to allow cloudformation:* on all resources. Add a policy that allows the iam:PassRole action for the ARN of the CloudFormationDeployment role if iam:PassedToService equals cloudformation.amazonaws.com.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
A company hosts a security auditing application in an AWS account. The auditing application uses an IAM role to access other AWS accounts. All the accounts are in the same organization in AWS Organizations.A recent security audit revealed that users in the audited AWS accounts could modify or delete the auditing application's IAM role. The company needs to prevent any modification to the auditing application's IAM role by any entity other than a trusted administrator IAM role.Which solution will meet these requirements?

A. Create an SCP that includes a Deny statement for changes to the auditing application's IAM role. Include a condition that allows the trusted administrator IAM role to make changes. Attach the SCP to the root of the organization.

B. Create an SCP that includes an Allow statement for changes to the auditing application's IAM role by the trusted administrator IAM role. Include a Deny statement for changes by all other IAM principals. Attach the SCP to the IAM service in each AWS account where the auditing application has an IAM role.
C. Create an IAM permissions boundary that includes a Deny statement for changes to the auditing application's IAM role. Include a condition that allows the trusted administrator IAM role to make changes. Attach the permissions boundary to the audited AWS accounts.
D. Create an IAM permissions boundary that includes a Deny statement for changes to the auditing applicationâ€™s IAM role. Include a condition that allows the trusted administrator IAM role to make changes. Attach the permissions boundary to the auditing application's IAM role in the AWS accounts.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
A company is developing a web application's infrastructure using AWS CloudFormation. The database engineering team maintains the database resources in a CloudFormation template, and the software development team maintains the web application resources in a separate CloudFormation template. As the scope of the application grows, the software development team needs to use resources maintained by the database engineering team. However, both teams have their own review and lifecycle management processes that they want to keep. Both teams also require resource-level change-set reviews. The software development team would like to deploy changes to this template using their CI/CD pipeline.Which solution will meet these requirements?

A. Create a stack export from the database CloudFormation template and import those references into the web application CloudFormation template.
B. Create a CloudFormation nested stack to make cross-stack resource references and parameters available in both stacks.
C. Create a CloudFormation stack set to make cross-stack resource references and parameters available in both stacks.
D. Create input parameters in the web application CloudFormation template and pass resource names and IDs from the database stack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
A company has an organization in AWS Organizations. A DevOps engineer needs to maintain multiple AWS accounts that belong to different OUs in the organization. All resources, including IAM policies and Amazon S3 policies within an account, are deployed through AWS CloudFormation. All templates and code are maintained in an AWS CodeCommit repository. Recently, some developers have not been able to access an S3 bucket from some accounts in the organization.The following policy is attached to the S3 bucket:What should the DevOps engineer do to resolve this access issue?

A. Modify the S3 bucket policy. Turn off the S3 Block Public Access setting on the S3 bucket. In the S3 policy, add the aws:SourceAccount condition. Add the AWS account IDs of all developers who are experiencing the issue.
B. Verify that no IAM permissions boundaries are denying developers access to the S3 bucket. Make the necessary changes to IAM permissions boundaries. Use an AWS Config recorder in the individual developer accounts that are experiencing the issue to revert any changes that are blocking access. Commit

the fix back into the CodeCommit repository. Invoke deployment through CloudFormation to apply the changes.

C. Configure an SCP that stops anyone from modifying IAM resources in developer OUs. In the S3 policy, add the aws:SourceAccount condition. Add the AWS account IDs of all developers who are experiencing the issue. Commit the fix back into the CodeCommit repository. Invoke deployment through CloudFormation to apply the changes.

D. Ensure that no SCP is blocking access for developers to the S3 bucket. Ensure that no IAM policy permissions boundaries are denying access to developer IAM users. Make the necessary changes to the SCP and IAM policy permissions boundaries in the CodeCommit repository. Invoke deployment through CloudFormation to apply the changes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
A company has an organization in AWS Organizations for its multi-account environment. A DevOps engineer is developing an AWS CodeArtifact based strategy for application package management across the organization. Each application team at the company has its own account in the organization. Each application team also has limited access to a centralized shared services account.Each application team needs full access to download, publish, and grant access to its own packages. Some common library packages that the application teams use must also be shared with the entire organization.Which combination of steps will meet these requirements with the LEAST administrative overhead? (Choose three.)

A. Create a domain in each application team's account. Grant each application team's account full read access and write access to the application team's domain.

B. Create a domain in the shared services account. Grant the organization read access and CreateRepository access.

C. Create a repository in each application teamâ€™s account. Grant each application teamâ€™s account full read access and write access to its own repository.

D. Create a repository in the shared services account. Grant the organization read access to the repository in the shared services account Set the repository as the upstream repository in each application team's repository.

E. For teams that require shared packages, create resource-based policies that allow read access to the repository from other application teams' accounts.

F. Set the other application teams' repositories as upstream repositories.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
A company deploys an application to Amazon EC2 instances. The application runs Amazon Linux 2 and uses AWS CodeDeploy. The application has the following file structure for its code repository:The appspec.yml file has the following contents in the files section:What will the result be for the deployment of the config.txt file?

A. The config.txt file will be deployed to only /var/www/html/config/config.txt.

B. The config.txt file will be deployed to /usr/local/src/config.txt and to /var/www/html/config/config.txt.

C. The config.txt file will be deployed to only /usr/local/src/config.txt.

D. The config.txt file will be deployed to /usr/local/src/config.txt and to /var/www/html/application/web/config.txt.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
A company has set up AWS CodeArtifact repositories with public upstream repositories. The company's development team consumes open source dependencies from the repositories in the company's internal network.The company's security team recently discovered a critical vulnerability in the most recent version of a package that the development team consumes. The security team has produced a patched version to fix the vulnerability. The company needs to prevent the vulnerable version from being downloaded. The company also needs to allow the security team to publish the patched version.Which combination of steps will meet these requirements? (Choose two.)

A. Update the status of the affected CodeArtifact package version to unlisted.
B. Update the status of the affected CodeArtifact package version to deleted.
C. Update the status of the affected CodeArtifact package version to archived.
D. Update the CodeArtifact package origin control settings to allow direct publishing and to block upstream operations.
E. Update the CodeArtifact package origin control settings to block direct publishing and to allow upstream operations.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
A company is running a custom-built application that processes records. All the components run on Amazon EC2 instances that run in an Auto Scaling group. Each record's processing is a multistep sequential action that is compute-intensive. Each step is always completed in 5 minutes or less.A limitation of the current system is that if any steps fail, the application has to reprocess the record from the beginning. The company wants to update the architecture so that the application must reprocess only the failed steps.What is the MOST operationally efficient solution that meets these requirements?

A. Create a web application to write records to Amazon S3. Use S3 Event Notifications to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Use an EC2 instance to poll Amazon SNS and start processing. Save intermediate results to Amazon S3 to pass on to the next step.
B. Perform the processing steps by using logic in the application. Convert the application code to run in a container. Use AWS Fargate to manage the container instances. Configure the container to invoke itself to pass the state from one step to the next.
C. Create a web application to pass records to an Amazon Kinesis data stream. Decouple the processing by using the Kinesis data stream and AWS Lambda functions.
D. Create a web application to pass records to AWS Step Functions. Decouple the processing into Step Functions tasks and AWS Lambda functions.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
A company is migrating its on-premises Windows applications and Linux applications to AWS. The company will use automation to launch Amazon EC2 instances to mirror the on-premises configurations. The migrated applications require access to shared storage that uses SMB for Windows and NFS for Linux.The company is also creating a pilot light disaster recovery (DR) environment in another AWS Region. The company will use automation to launch and configure the EC2 instances in the DR Region. The company needs to replicate the storage to the DR Region.Which storage solution will meet these requirements?

A. Use Amazon S3 for the application storage. Create an S3 bucket in the primary Region and an S3 bucket in the DR Region. Configure S3 Cross-Region Replication (CRR) from the primary Region to the DR Region.
B. Use Amazon Elastic Block Store (Amazon EBS) for the application storage. Create a backup plan in AWS Backup that creates snapshots of the EBS volumes that are in the primary Region and replicates the snapshots to the DR Region.
C. Use a Volume Gateway in AWS Storage Gateway for the application storage. Configure Cross-Region Replication (CRR) of the Volume Gateway from the primary Region to the DR Region.
D. Use Amazon FSx for NetApp ONTAP for the application storage. Create an FSx for ONTAP instance in the DR Region. Configure NetApp SnapMirror replication from the primary Region to the DR Region.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A company's application uses a fleet of Amazon EC2 On-Demand Instances to analyze and process data. The EC2 instances are in an Auto Scaling group. The Auto Scaling group is a target group for an Application Load Balancer (ALB). The application analyzes critical data that cannot tolerate interruption. The application also analyzes noncritical data that can withstand interruption.The critical data analysis requires quick scalability in response to real-time application demand. The noncritical data analysis involves memory consumption. A DevOps engineer must implement a solution that reduces scale-out latency for the critical data. The solution also must process the noncritical data.Which combination of steps will meet these requirements? (Choose two.)

A. For the critical data, modify the existing Auto Scaling group. Create a warm pool instance in the stopped state. Define the warm pool size. Create a new version of the launch template that has detailed monitoring enabled. Use Spot Instances.
B. For the critical data, modify the existing Auto Scaling group. Create a warm pool instance in the stopped state. Define the warm pool size. Create a new version of the launch template that has detailed monitoring enabled. Use On-Demand Instances.
C. For the critical data, modify the existing Auto Scaling group. Create a lifecycle hook to ensure that bootstrap scripts are completed successfully. Ensure that the application on the instances is ready to accept traffic before the instances are registered. Create a new version of the launch template that has detailed monitoring enabled.
D. For the noncritical data, create a second Auto Scaling group that uses a launch template. Configure the launch template to install the unified Amazon CloudWatch agent and to configure the CloudWatch agent with a custom memory utilization metric. Use Spot Instances. Add the new Auto Scaling group as the target group for the AL
E. For the noncritical data, create a second Auto Scaling group. Choose the predefined memory utilization metric type for the target tracking scaling policy. Use Spot Instances. Add the new Auto Scaling group as the target group for the AL

Correct Answer: BDB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A company recently migrated its application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that uses Amazon EC2 instances. The company configured the application to automatically scale based on CPU utilization.The application produces memory errors when it experiences heavy loads. The application also does not scale out enough to handle the increased load. The company needs to collect and analyze memory metrics for the application over time.Which combination of steps will meet these requirements? (Choose three.)

A. Attach the CloudWatchAgentServerPolicy managed IAM policy to the IAM instance profile that the cluster uses.
B. Attach the CloudWatchAgentServerPolicy managed IAM policy to a service account role for the cluster.
C. Collect performance metrics by deploying the unified Amazon CloudWatch agent to the existing EC2 instances in the cluster. Add the agent to the AMI for any new EC2 instances that are added to the cluster.
D. Collect performance logs by deploying the AWS Distro for OpenTelemetry collector as a DaemonSet.
E. Analyze the pod_memory_utilization Amazon CloudWatch metric in the ContainerInsights namespace by using the Service dimension.
F. Analyze the node_memory_utilization Amazon CloudWatch metric in the ContainerInsights namespace by using the ClusterName dimension.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
A company's video streaming platform usage has increased from 10,000 users each day to 50,000 users each day in multiple countries. The company deploys the streaming platform on Amazon Elastic Kubernetes Service (Amazon EKS). The EKS workload scales up to thousands of nodes during peak viewing time.The company's users report occurrences of unauthorized logins. Users also report sudden interruptions and logouts from the platform.The company wants additional security measures for the entire platform. The company also needs a summarized view of the resource behaviors and interactions across the company's entire AWS environment. The summarized view must show login attempts, API calls, and network traffic. The solution must permit network traffic analysis while minimizing the overhead of managing logs. The solution must also quickly investigate any potential malicious behavior that is associated with the EKS workload.Which solution will meet these requirements?

A. Enable Amazon GuardDuty for EKS Audit Log Monitoring. Enable AWS CloudTrail logs. Store the EKS audit logs and CloudTrail log files in an Amazon S3 bucket. Use Amazon Athena to create an external table. Use Amazon QuickSight to create a dashboard.
B. Enable Amazon GuardDuty for EKS Audit Log Monitoring. Enable Amazon Detective in the company's AWS account. Enable EKS audit logs from optional source packages in Detective.
C. Enable Amazon CloudWatch Container Insights. Enable AWS CloudTrail logs. Store the EKS audit logs and CloudTrail log files in an Amazon S3 bucket. Use Amazon Athena to create an external table. Use Amazon QuickSight to create a dashboard.
D. Enable Amazon GuardDuty for EKS Audit Log Monitoring. Enable Amazon CloudWatch Container Insights and VPC Flow Logs. Enable AWS CloudTrail logs.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
A company has an on-premises application that is written in Go. A DevOps engineer must move the application to AWS. The company's development team wants to enable blue/green deployments and perform A/B testing.Which solution will meet these requirements?

A. Deploy the application on an Amazon EC2 instance, and create an AMI of the instance. Use the AMI to create an automatic scaling launch configuration that is used in an Auto Scaling group. Use Elastic Load Balancing to distribute traffic. When changes are made to the application, a new AMI will be created, which will initiate an EC2 instance refresh.
B. Use Amazon Lightsail to deploy the application. Store the application in a zipped format in an Amazon S3 bucket. Use this zipped version to deploy new versions of the application to Lightsail. Use Lightsail deployment options to manage the deployment.
C. Use AWS CodeArtifact to store the application code. Use AWS CodeDeploy to deploy the application to a fleet of Amazon EC2 instances. Use Elastic Load Balancing to distribute the traffic to the EC2 instances. When making changes to the application, upload a new version to CodeArtifact and create a new CodeDeploy deployment.
D. Use AWS Elastic Beanstalk to host the application. Store a zipped version of the application in Amazon S3. Use that location to deploy new versions of the application. Use Elastic Beanstalk to manage the deployment options.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
A company uses AWS Organizations to manage hundreds of AWS accounts. The company has a team that is responsible for AWS Identity and Access Management (IAM).The IAM team wants to implement AWS IAM Identity Center (AWS Single Sign-On). The IAM team must have only the minimum needed permissions to manage IAM Identity Center. The IAM team must not be able to gain unneeded access to the Organizations management account. The IAM team must be able to provision new IAM Identity Center permission sets and assignments for existing and new member accounts.Which combination of steps will meet these requirements? (Choose three.)

A. Create a new AWS account for the IAM team. In the new account, enable IAM Identity Center. In the Organizations management account, register the new account as a delegated administrator for IAM Identity Center.
B. Create a new AWS account for the IAM team. In the Organizations management account, enable IAM Identity Center. In the Organizations management account, register the new account as a delegated administrator for IAM Identity Center.
C. In IAM Identity Center, create users and a group for the IAM team. Add the users to the group. Create a new permission set. Attach the AWSSSODirectoryAdministrator managed IAM policy to the group.
D. In IAM Identity Center, create users and a group for the IAM team. Add the users to the group. Create a new permission set. Attach the AWSSSOMemberAccountAdministrator managed IAM policy to the group.
E. Assign the permission set to the Organizations management account. Allow the IAM team group to use the permission set.
F. Assign the permission set to the new AWS account. Allow the IAM team group to use the permission set.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A company uses an organization in AWS Organizations that has all features enabled. The company uses AWS Backup in a primary account and uses an AWS Key Management Service (AWS KMS) key to encrypt the backups.The company needs to automate a cross-account backup of the resources that AWS Backup backs up in the primary account. The company configures cross-account backup in the Organizations management account. The company creates a new AWS account in the organization and configures an AWS Backup backup vault in the new account. The company creates a KMS key in the new account to encrypt the backups. Finally, the company configures a new backup plan in the primary account. The destination for the new backup plan is the backup vault in the new account.When the AWS Backup job in the primary account is invoked, the job creates backups in the primary account. However, the backups are not copied to the new account's backup vault.Which combination of steps must the company take so that backups can be copied to the new account's backup vault? (Choose two.)

A. Edit the backup vault access policy in the new account to allow access to the primary account.
B. Edit the backup vault access policy in the primary account to allow access to the new account.
C. Edit the backup vault access policy in the primary account to allow access to the KMS key in the new account.
D. Edit the key policy of the KMS key in the primary account to share the key with the new account.
E. Edit the key policy of the KMS key in the new account to share the key with the primary account.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A company runs an application that uses an Amazon S3 bucket to store images. A DevOps engineer needs to implement a multi-Region strategy for the objects that are stored in the S3 bucket. The company needs to be able to fail over to an S3 bucket in another AWS Region. When an image is added to either S3 bucket, the image must be replicated to the other S3 bucket within 15 minutes.The DevOps engineer enables two-way replication between the S3 buckets.Which combination of steps should the DevOps engineer take next to meet the requirements? (Choose three.)

A. Enable S3 Replication Time Control (S3 RTC) on each replication rule.
B. Create an S3 Multi-Region Access Point in an active-passive configuration.
C. Call the SubmitMultiRegionAccessPointRoutes operation in the AWS API when the company needs to fail over to the S3 bucket in the other Region.
D. Enable S3 Transfer Acceleration on both S3 buckets.
E. Configure a routing control in Amazon Route 53 Recovery Controller. Add the S3 buckets in an active-passive configuration.
F. Call the UpdateRoutingControlStates operation in the AWS API when the company needs to fail over to the S3 bucket in the other Region.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
A company uses the AWS Cloud Development Kit (AWS CDK) to define its application. The company uses a

pipeline that consists of AWS CodePipeline and AWS CodeBuild to deploy the CDK application.The company wants to introduce unit tests to the pipeline to test various infrastructure components. The company wants to ensure that a deployment proceeds if no unit tests result in a failure.Which combination of steps will enforce the testing requirement in the pipeline? (Choose two.)

A. Update the CodeBuild build phase commands to run the tests then to deploy the application. Set the OnFailure phase property to ABOR
B. Update the CodeBuild build phase commands to run the tests then to deploy the application. Add the --rollback true flag to the cdk deploy command.
C. Update the CodeBuild build phase commands to run the tests then to deploy the application. Add the --require-approval any-change flag to the cdk deploy command.
D. Create a test that uses the AWS CDK assertions module. Use the template.hasResourceProperties assertion to test that resources have the expected properties.
E. Create a test that uses the cdk diff command. Configure the test to fail if any resources have changed.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
A company has an application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances are in multiple Availability Zones. The application was misconfigured in a single Availability Zone, which caused a partial outage of the application.A DevOps engineer made changes to ensure that the unhealthy EC2 instances in one Availability Zone do not affect the healthy EC2 instances in the other Availability Zones. The DevOps engineer needs to test the application's failover and shift where the ALB sends traffic. During failover, the ALB must avoid sending traffic to the Availability Zone where the failure has occurred.Which solution will meet these requirements?

A. Turn off cross-zone load balancing on the AL
B. Use Amazon Route 53 Application Recovery Controller to start a zonal shift away from the Availability Zone.
C. Create an Amazon Route 53 Application Recovery Controller resource set that uses the DNS hostname of the AL
D. Create an Amazon Route 53 Application Recovery Controller resource set that uses the ARN of the ALBâ €™s target group. Create a readiness check that uses the ElbV2TargetGroupsCanServeTraffic rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
A company sends its AWS Network Firewall flow logs to an Amazon S3 bucket. The company then analyzes the flow logs by using Amazon Athena.The company needs to transform the flow logs and add additional data before the flow logs are delivered to the existing S3 bucket.Which solution will meet these requirements?

A. Create an AWS Lambda function to transform the data and to write a new object to the existing S3 bucket. Configure the Lambda function with an S3 trigger for the existing S3 bucket. Specify all object create events for the event type. Acknowledge the recursive invocation.
B. Enable Amazon EventBridge notifications on the existing S3 bucket. Create a custom EventBridge event bus. Create an EventBridge rule that is associated with the custom event bus. Configure the rule to react to all object create events for the existing S3 bucket and to invoke an AWS Step Functions workflow. Configure a Step Functions task to transform the data and to write the data into a new S3 bucket.

C. Create an Amazon EventBridge rule that is associated with the default EventBridge event bus. Configure the rule to react to all object create events for the existing S3 bucket. Define a new S3 bucket as the target for the rule. Create an EventBridge input transformation to customize the event before passing the event to the rule target.
D. Create an Amazon Kinesis Data Firehose delivery stream that is configured with an AWS Lambda transformer. Specify the existing S3 bucket as the destination. Change the Network Firewall logging destination from Amazon S3 to Kinesis Data Firehose.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
A DevOps engineer needs to implement integration tests into an existing AWS CodePipeline CI/CD workflow for an Amazon Elastic Container Service (Amazon ECS) service. The CI/CD workflow retrieves new application code from an AWS CodeCommit repository and builds a container image. The CI/CD workflow then uploads the container image to Amazon Elastic Container Registry (Amazon ECR) with a new image tag version.The integration tests must ensure that new versions of the service endpoint are reachable and that various API methods return successful response data. The DevOps engineer has already created an ECS cluster to test the service.Which combination of steps will meet these requirements with the LEAST management overhead? (Choose three.)

A. Add a deploy stage to the pipeline. Configure Amazon ECS as the action provider.
B. Add a deploy stage to the pipeline. Configure AWS CodeDeploy as the action provider.
C. Add an appspec.yml file to the CodeCommit repository.
D. Update the image build pipeline stage to output an imagedefinitions.json file that references the new image tag.
E. Create an AWS Lambda function that runs connectivity checks and API calls against the service. Integrate the Lambda function with CodePipeline by using a Lambda action stage.
F. Write a script that runs integration tests against the service. Upload the script to an Amazon S3 bucket. Integrate the script in the S3 bucket with CodePipeline by using an S3 action stage.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
A company runs applications on Windows and Linux Amazon EC2 instances. The instances run across multiple Availability Zones in an AWS Region. The company uses Auto Scaling groups for each application.The company needs a durable storage solution for the instances. The solution must use SMB for Windows and must use NFS for Linux. The solution must also have sub-millisecond latencies. All instances will read and write the data.Which combination of steps will meet these requirements? (Choose three.)

A. Create an Amazon Elastic File System (Amazon EFS) file system that has targets in multiple Availability Zones.
B. Create an Amazon FSx for NetApp ONTAP Multi-AZ file system.
C. Create a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume to use for shared storage.
D. Update the user data for each applicationâ€™s launch template to mount the file system.
E. Perform an instance refresh on each Auto Scaling group.

F. Update the EC2 instances for each application to mount the file system when new instances are launched.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
A company uses an organization in AWS Organizations that a security team and a DevOps team manage. Both teams access the accounts by using AWS IAM Identity Center.A dedicated group has been created for each team. The DevOps team's group has been assigned a permission set named DevOps. The permission set has the AdministratorAccess managed IAM policy attached. The permission set has been applied to all accounts in the organization.The security team wants to ensure that the DevOps team does not have access to IAM Identity Center in the organization's management account. The security team has attached the following SCP to the organization root:After implementing the policy, the security team discovers that the DevOps team can still access IAM Identity Center.Which solution will fix the problem?

A. In the organization's management account, create a new O
B. In the organization's management account, update the SCP condition reference to the ARN of the DevOps team's group role to include the AWS account ID of the organization's management account.
C. In IAM Identity Center, create a new permission set. Ensure that the assigned policy has full access but explicitly denies permission for the sso:* action and the sso-directory:* action. Update the assigned permission set for the DevOps team's group role in the organization's management account. Delete the SC
D. In IAM Identity Center, update the DevOps permission set. Ensure that the assigned policy has full access but explicitly denies permission for the sso:* action and the sso-directory:* action. In the Deny statement, add a StringEquals condition that compares the aws:SourceAccount global condition context key with the organization's management account IDelete the SC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
An Amazon EC2 Auto Scaling group manages EC2 instances that were created from an AMI. The AMI has the AWS Systems Manager Agent installed. When an EC2 instance is launched into the Auto Scaling group, tags are applied to the EC2 instance.EC2 instances that are launched by the Auto Scaling group must have the correct operating system configuration.Which solution will meet these requirements?

A. Create a Systems Manager Run Command document that configures the desired instance configuration. Set up Systems Manager Compliance to invoke the Run Command document when the EC2 instances are not in compliance with the most recent patches.
B. Create a Systems Manager State Manager association that links to the Systems Manager command document. Create a tag query that runs immediately.
C. Create a Systems Manager Run Command task that specifies the desired instance configuration. Create a maintenance window in Systems Manager Maintenance Windows that runs daily. Register the Run Command task against the maintenance window. Designate the targets.
D. Create a Systems Manager Patch Manager patch baseline and a patch group that use the same tags that the Auto Scaling group applies. Register the patch group with the patch baseline. Define a Systems Manager command document to patch the instances Invoke the document by using Systems Manager Run Command.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
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 invokes 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 an AWS Config rule for EC2 Instance-terminate Lifecycle Action and trigger a step function that invokes 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 invokes a script to collect 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 EventBridge rule for EC2 Instance-terminate Lifecycle Action and trigger an AWS Lambda function that invokes an SSM Run Command script to collect logs, push them to Amazon S3, and complete the lifecycle action once logs are collected.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
A company uses AWS Organizations to manage its AWS accounts. The organization root has a child OU that is named Department. The Department OU has a child OU that is named Engineering. The default FullAWSAccess policy is attached to the root, the Department OU, and the Engineering OU.The company has many AWS accounts in the Engineering OU. Each account has an administrative IAM role with the AdministratorAccess IAM policy attached. The default FullAWSAccessPolicy is also attached to each account.A DevOps engineer plans to remove the FullAWSAccess policy from the Department OU. The DevOps engineer will replace the policy with a policy that contains an Allow statement for all Amazon EC2 API operations.What will happen to the permissions of the administrative 1AM roles as a result of this change?

A. All API actions on all resources will be allowed.
B. All API actions on EC2 resources will be allowed. All other API actions will be denied.
C. All API actions on all resources will be denied.
D. All API actions on EC2 resources will be denied. All other API actions will be allowed.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
A company manages AWS accounts in AWS Organizations. The company needs a solution to send Amazon CloudWatch Logs data to an Amazon S3 bucket in a dedicated AWS account. The solution must support all existing and future CloudWatch Logs log groups.Which solution will meet these requirements?

A. Enable Organizations backup policies to back up all log groups to a dedicated S3 bucket. Add an S3 bucket policy that allows access from all accounts that belong to the company.
B. Create a backup plan in AWS Backup. Specify a dedicated S3 bucket as a backup vault. Assign all CloudWatch Logs log group resources to the backup plan. Create resource assignments in the backup plan for all accounts that belong to the company.
C. Create a backup plan in AWS Backup. Specify a dedicated S3 bucket as a backup vault. Assign all existing log groups to the backup plan. Create resource assignments in the backup plan for all accounts that belong to the company. Create an AWS Systems Manager Automation runbook to assign log groups to a backup plan. Create an AWS Config rule that has an automatic remediation action for all noncompliant log groups. Specify the runbook as the rule's target.
D. Create a CloudWatch Logs destination and an Amazon Kinesis Data Firehose delivery stream in the dedicated AWS account. Specify the S3 bucket as the destination of the delivery stream. Create subscription filters for all existing log groups in all accounts. Create an AWS Lambda function to call the CloudWatch Logs PutSubscriptionFilter API operation. Create an Amazon EventBridge rule to invoke the Lambda function when a CreateLogGroup event occurs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
A DevOps engineer manages a Java-based application that runs in an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate. Auto scaling has not been configured for the application.The DevOps engineer has determined that the Java Virtual Machine (JVM) thread count is a good indicator of when to scale the application. The application serves customer traffic on port 8080 and makes JVM metrics available on port 9404.Application use has recently increased. The DevOps engineer needs to configure auto scaling for the application.Which solution will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Deploy the Amazon CloudWatch agent as a container sidecar. Configure the CloudWatch agent to retrieve JVM metrics from port 9404. Create CloudWatch alarms on the JVM thread count metric to scale the application. Add a step scaling policy in Fargate to scale up and scale down based on the CloudWatch alarms.
B. Deploy the Amazon CloudWatch agent as a container sidecar. Configure a metric filter for the JVM thread count metric on the CloudWatch log group for the CloudWatch agent. Add a target tracking policy in Fargate. Select the metric from the metric filter as a scale target.
C. Create an Amazon Managed Service for Prometheus workspace. Deploy AWS Distro for OpenTelemetry as a container sidecar to publish the JVM metrics from port 9404 to the Prometheus workspace. Configure rules for the workspace to use the JVM thread count metric to scale the application. Add a step scaling policy in Fargate. Select the Prometheus rules to scale up and scaling down.
D. Create an Amazon Managed Service for Prometheus workspace. Deploy AWS Distro for OpenTelemetry as a container sidecar to retrieve JVM metrics from port 9404 to publish the JVM metrics from port 9404 to the Prometheus workspace. Add a target tracking policy in Fargate. Select the Prometheus metric as a scale target.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
A company has an application that runs in a single AWS Region. The application runs on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster and connects to an Amazon Aurora MySQL cluster. The application is built in an AWS CodeBuild project. The container images are published to Amazon Elastic Container Registry (Amazon ECR).The company needs to replicate the state of the application for the container images and the database to a second Region.Which solution will meet these requirements in the MOST operationally efficient way?

A. Turn on Amazon S3 Cross-Region Replication (CRR) on the bucket that holds the ECR container images. Deploy the application to an EKS cluster in the second Region by referencing the new S3 bucket object URL for the container image in a Kubernetes deployment file. Configure a cross-Region Aurora Replica in the second Region. Configure the new application deployment to use the endpoints for the cross-Region Aurora Replica.
B. Create an Amazon EventBridge rule that reacts to image pushes to the ECR repository. Configure the EventBridge rule to invoke an AWS Lambda function to replicate the image to a new ECR repository in the second Region. Deploy the application to an EKS cluster in the second Region by referencing the new ECR repository in a Kubernetes deployment file. Configure a cross-Region Aurora Replica in the second Region. Configure the new application deployment to use the endpoints for the cross-Region Aurora Replica.
C. Turn on Cross-Region Replication to replicate the ECR repository to the second Region. Deploy the application to an EKS cluster in the second Region by referencing the new ECR repository in a Kubernetes deployment file. Configure an Aurora global database with clusters in the initial Region and the second Region. Configure the new application deployment to use the endpoints for the second Region's cluster in the Aurora global database.
D. Configure the CodeBuild project to also push the container image to an ECR repository in the second Region. Deploy the application to an EKS cluster in the second Region by referencing the new ECR repository in a Kubernetes deployment file. Configure an Aurora MySQL cluster in the second Region as the target for binary log replication from the Aurora MySQL cluster in the initial Region. Configure the new application deployment to use the endpoints for the second Region's cluster.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
A company is building a serverless application that uses AWS Lambda functions to process data.A BeginResponse Lambda function initializes data in response to specific application events. The company needs to ensure that a large number of Lambda functions are invoked after the BeginResponse Lambda function runs. Each Lambda function must be invoked in parallel and depends on only the outputs of the BeginResponse Lambda function. Each Lambda function has retry logic for invocation and must be able to fine-tune concurrency without losing data.Which solution will meet these requirements with the MOST operational efficiency?

A. Create an Amazon Simple Notification Service (Amazon SNS) topic. Modify the BeginResponse Lambda function to publish to the SNS topic before the BeginResponse Lambda function finishes running. Subscribe all Lambda functions that need to invoke after the BeginResponse Lambda function runs to the SNS topic. Subscribe any new Lambda functions to the SNS topic.
B. Create an Amazon Simple Queue Service (Amazon SQS) queue for each Lambda function that needs to run after the BeginResponse Lambda function runs. Subscribe each Lambda function to its own SQS queue. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe each SQS queue to the SNS topic. Modify the BeginResponse function to publish to the SNS topic when it finishes running.
C. Create an Amazon Simple Queue Service (Amazon SQS) queue for each Lambda function that needs to run after the BeginResponse Lambda function runs. Subscribe the Lambda function to the SQS queue. Create an Amazon Simple Notification Service (Amazon SNS) topic for each SQS queue. Subscribe the

SQS queues to the SNS topics. Modify the BeginResponse function to publish to the SNS topics when the function finishes running.

D. Create an AWS Step Functions Standard Workflow. Configure states in the workflow to invoke the Lambda functions sequentially. Create an Amazon Simple Notification Service (Amazon SNS) topic. Modify the BeginResponse Lambda function to publish to the SNS topic before the Lambda function finishes running. Create a new Lambda function that is subscribed to the SNS topic and that invokes the Step Functions workflow.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
A company operates a globally deployed product out of multiple AWS Regions. The company's DevOps team needs to use Amazon API Gateway to deploy an API to support the product.The API must be deployed redundantly. The deployment must provide independent availability from each company location. The deployment also must respond to a custom domain URL and must optimize performance for the API user requests.Which solution will meet these requirements?

A. Deploy an API Gateway edge-optimized API endpoint in the us-east-1 Region. Create an API Gateway custom domain for the AP
B. Deploy an API Gateway regional API endpoint in the us-east-1 Region. Integrate the API Gateway API with a public Application Load Balancer (ALB). Create an AWS Global Accelerator standard accelerator. Associate the endpoint with the ALCreate an Amazon Route 53 alias record set that points the custom domain name to the DNS name that is assigned to the accelerator.
C. Deploy an API Gateway regional API endpoint in every AWS Region where the company's product is deployed. Create an API Gateway custom domain in each Region for the deployed API Gateway AP
D. Deploy an API Gateway edge-optimized API endpoint in the us-east-1 Region. Create an Amazon CloudFront distribution. Configure the CloudFront distribution with an alternate domain name. Specify the API Gateway Invoke URL as the origin domain. Create an Amazon Route 53 alias record set with a simple routing policy. Point the routing policy to the CloudFront distribution domain name.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
A DevOps engineer uses AWS CodeBuild to frequently produce software packages. The CodeBuild project builds large Docker images that the DevOps engineer can use across multiple builds.The DevOps engineer wants to improve build performance and minimize costs.Which solution will meet these requirements?

A. Store the Docker images in an Amazon Elastic Container Registry (Amazon ECR) repository. Implement a local Docker layer cache for CodeBuild.
B. Cache the Docker images in an Amazon S3 bucket that is available across multiple build hosts. Expire the cache by using an S3 Lifecycle policy.
C. Store the Docker images in an Amazon Elastic Container Registry (Amazon ECR) repository. Modify the CodeBuild project runtime configuration to always use the most recent image version.
D. Create custom AMIs that contain the cached Docker images. In the CodeBuild build, launch Amazon EC2 instances from the custom AMIs.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
A large company recently acquired a small company. The large company invited the small company to join the large company's existing organization in AWS Organizations as a new OU.A DevOps engineer determines that the small company needs to launch t3.small Amazon EC2 instance types for the company's application workloads. The small company needs to deploy the instances only within US-based AWS Regions.The DevOps engineer needs to use an SCP in the small company's new OU to ensure that the small company can launch only the required instance types.Which solution will meet these requirements?

A. Configure a statement to deny the ec2:RunInstances action for all EC2 instance resources when the ec2:InstanceType condition is not equal to t3.small.

   Configure another statement to deny the ec2:RunInstances action for all EC2 instance resources when the aws:RequestedRegion condition is not equal to us-*.
B. Configure a statement to allow the ec2:RunInstances action for all EC2 instance resources when the ec2:InstanceType condition is not equal to t3.small.

   Configure another statement to allow the ec2:RunInstances action for all EC2 instance resources when the aws:RequestedRegion condition is not equal to us-*.
C. Configure a statement to deny the ec2:RunInstances action for all EC2 instance resources when the ec2:InstanceType condition is equal to t3.small.

   Configure another statement to deny the ec2:RunInstances action for all EC2 instance resources when the aws:RequestedRegion condition is equal to us-*.
D. Configure a statement to allow the ec2:RunInstances action for all EC2 instance resources when the ec2:InstanceType condition is equal to t3.small.

   Configure another statement to allow the ec2:RunInstances action for all EC2 instance resources when the aws:RequestedRegion condition is equal to us-*.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
A DevOps team manages infrastructure for an application. The application uses long-running processes to process items from an Amazon Simple Queue Service (Amazon SQS) queue. The application is deployed to an Auto Scaling group.The application recently experienced an issue where items were taking significantly longer to process. The queue exceeded the expected size, which prevented various business processes from functioning properly. The application records all logs to a third-party tool.The team is currently subscribed to an Amazon Simple Notification Service (Amazon SNS) topic that the team uses for alerts. The team needs to be alerted if the queue exceeds the expected size.Which solution will meet these requirements with the MOST operational efficiency?

A. Create an Amazon CloudWatch metric alarm with a period of 1 hour and a static threshold to alarm if the average of the ApproximateNumberOfMessagesDelayed metric is greater than the expected value. Configure the alarm to notify the SNS topic.
B. Create an Amazon CloudWatch metric alarm with a period of 1 hour and a static threshold to alarm if the sum of the ApproximateNumberOfMessagesVisible metric is greater than the expected value. Configure the alarm to notify the SNS topic.

C. Create an AWS Lambda function that retrieves the ApproximateNumberOfMessages SQS queue attribute value and publishes the value as a new CloudWatch custom metric. Create an Amazon EventBridge rule that is scheduled to run every 5 minutes and that invokes the Lambda function. Configure a CloudWatch metrics alarm with a period of 1 hour and a static threshold to alarm if the sum of the new custom metric is greater than the expected value.
D. Create an AWS Lambda function that checks the ApproximateNumberOfMessagesDelayed SQS queue attribute and compares the value to a defined expected size in the function. Create an Amazon EventBridge rule that is scheduled to run every 5 minutes and that invokes the Lambda function. When the ApproximateNumberOfMessagesDelayed SQS queue attribute exceeds the expected size, send a notification the SNS topic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
A large company runs critical workloads in multiple AWS accounts. The AWS accounts are managed under AWS Organizations with all features enabled. The company stores confidential customer data in an Amazon S3 bucket. Access to the S3 bucket requires multiple levels of approval.The company wants to monitor when the S3 bucket is accessed by using the AWS CLI. The company also wants insights into the various activities performed by other users on all other S3 buckets in the AWS accounts to detect any issues.Which solution will meet these requirements?

A. Create an AWS CloudTrail trail that is delivered to Amazon CloudWatch in each AWS account. Enable data events logs for all S3 buckets. Use Amazon GuardDuty for anomaly detection in all the AWS accounts. Use Amazon Athena to perform SQL queries on the custom metrics created from the CloudTrail logs.
B. Create an AWS CloudTrail organization trail that is delivered to Amazon CloudWatch in the Organizations management account. Enable data events logs for all S3 buckets. Use Amazon CloudWatch anomaly detection in all the AWS accounts. Use Amazon Athena to perform SQL queries on the custom metrics created from the CloudTrail logs.
C. Create an AWS CloudTrail organization trail that is delivered to Amazon CloudWatch in the Organizations management account. Enable data events logs for all S3 buckets. Use Amazon CloudWatch anomaly detection in all the AWS accounts. Use Amazon CloudWatch Metrics Insights to perform SQL queries on the custom metrics created from the CloudTrail logs.
D. Create an AWS CloudTrail trail that is delivered to Amazon CloudWatch in each AWS account. Enable data events logs for all S3 buckets. Use a custom solution for anomaly detection in all the AWS accounts. Use Amazon CloudWatch Metrics Insights to perform SQL queries on the custom metrics created from the CloudTrail logs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
A company has an organization in AWS Organizations. The organization includes workload accounts that contain enterprise applications. The company centrally manages users from an operations account. No users can be created in the workload accounts. The company recently added an operations team and must provide the operations team members with administrator access to each workload account.Which combination of actions will provide this access? (Choose three.)

A. Create a SysAdmin role in the operations account. Attach the AdministratorAccess policy to the role. Modify the trust relationship to allow the sts:AssumeRole action from the workload accounts.

B. Create a SysAdmin role in each workload account. Attach the AdministratorAccess policy to the role. Modify the trust relationship to allow the sts:AssumeRole action from the operations account.
C. Create an Amazon Cognito identity pool in the operations account. Attach the SysAdmin role as an authenticated role.
D. In the operations account, create an IAM user for each operations team member.
E. In the operations account, create an IAM user group that is named SysAdmins. Add an IAM policy that allows the sts:AssumeRole action for the SysAdmin role in each workload account. Add all operations team members to the group.
F. Create an Amazon Cognito user pool in the operations account. Create an Amazon Cognito user for each operations team member.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
A DevOps team is deploying microservices for an application on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The cluster uses managed node groups. The DevOps team wants to enable auto scaling for the microservice Pods based on a specific CPU utilization percentage. The DevOps team has already installed the Kubernetes Metrics Server on the cluster.Which solution will meet these requirements in the MOST operationally efficient way?

A. Edit the Auto Scaling group that is associated with the worker nodes of the EKS cluster. Configure the Auto Scaling group to use a target tracking scaling policy to scale when the average CPU utilization of the Auto Scaling group reaches a specific percentage.
B. Deploy the Kubernetes Horizontal Pod Autoscaler (HPA) and the Kubernetes Vertical Pod Autoscaler (VPA) in the cluster. Configure the HPA to scale based on the target CPU utilization percentage. Configure the VPA to use the recommender mode setting.
C. Run the AWS Systems Manager AWS-UpdateEKSManagedNodeGroup Automation document. Modify the values for NodeGroupDesiredSize, NodeGroupMaxSize, and NodeGroupMinSize to be based on an estimate for the required node size.
D. Deploy the Kubernetes Horizontal Pod Autoscaler (HPA) and the Kubernetes Cluster Autoscaler in the cluster. Configure the HPA to scale based on the target CPU utilization percentage. Configure the Cluster Autoscaler to use the auto-discovery setting.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
A company has multiple AWS accounts. The company uses AWS IAM Identity Center that is integrated with a third-party SAML 2.0 identity provider (IdP).The attributes for access control feature is enabled in IAM Identity Center. The attribute mapping list maps the department key from the IdP to the ${path:enterprise.department} attribute. All existing Amazon EC2 instances have a d1, d2, d3 department tag that corresponds to three companyâ€™s departments.A DevOps engineer must create policies based on the matching attributes. The policies must grant each user access to only the EC2 instances that are tagged with the userâ€™s respective department name.Which condition key should the DevOps engineer include in the custom permissions policies to meet these requirements?

A.
B.

C.
D.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
A security team wants to use AWS CloudTrail to monitor all actions and API calls in multiple accounts that are in the same organization in AWS Organizations. The security team needs to ensure that account users cannot turn off CloudTrail in the accounts.Which solution will meet this requirement?

A. Apply an SCP to all OUs to deny the cloudtrail:StopLogging action and the cloudtrail:DeleteTrail action.
B. Create IAM policies in each account to deny the cloudtrail:StopLogging action and the cloudtrail:DeleteTrail action.
C. Set up Amazon CloudWatch alarms to notify the security team when a user disables CloudTrail in an account.
D. Use AWS Config to automatically re-enable CloudTrail if a user disables CloudTrail in an account.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
A DevOps engineer needs to configure a blue/green deployment for an existing three-tier application. The application runs on Amazon EC2 instances and uses an Amazon RDS database. The EC2 instances run behind an Application Load Balancer (ALB) and are in an Auto Scaling group.The DevOps engineer has created launch templates, Auto Scaling groups, and ALB target groups for the blue environment and the green environment. Each target group specifies which application version, blue or green, will be loaded on the EC2 instances. An Amazon Route 53 record for www.example.com points to the ALB.The deployment must shift traffic all at once from the blue environment to the green environment.Which solution will meet these requirements?

A. Starta rolling restart of the Auto Scaling group for the green environment to deploy the new application version to the green environment's EC2 instances. When the rolling restart is complete, use an AWS CLI command to update the ALB to send traffic to the green environment's target group.
B. Use an AWS CLI command to update the ALB to send traffic to the green environments target group. Start a rolling restart of the Auto Scaling group for the green environment to deploy the new application version to the green environment's EC2 instances.
C. Update the launch template to deploy the green environment's application version to the blue environment's EC2 instances. Do not change the target groups or the Auto Scaling groups in either environment. Perform a rolling restart of the blue environments EC2 instances.
D. Starta rolling restart of the Auto Scaling group for the green environment to deploy the new application version to the green environment's EC2 instances. When the rolling restart is complete, update Route 53 to point to the green environment's endpoint on the AL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
A company has an application that runs on Amazon EC2 instances in an Auto Scaling group. The application processes a high volume of messages from an Amazon Simple Queue Service (Amazon SQS) queue.A DevOps engineer noticed that the application took several hours to process a group of messages from the SQS queue. The average CPU utilization of the Auto Scaling group did not cross the threshold of a target tracking scaling policy when processing the messages. The application that processes the SQS queue publishes logs to â€˜Amazon CloudWatch Logs.The DevOps engineer needs to ensure that the queue is processed quickly.Which solution meets these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function. Configure the Lambda function to publish a custom metric by using the ApproximateNumberOfMessagesVisible SQS queue attribute and the GroupInServiceInstances Auto Scaling group attribute to publish the queue messages for each instance. Schedule an Amazon EventBridge rule to run the Lambda function every hour. Create a target tracking scaling policy for the Auto Scaling group that uses the custom metric to scale in and out.
B. Create an AWS Lambda function. Configure the Lambda function to publish a custom metric by using the ApproximateNumberOfMessagesVisible SQS queue attribute and the GroupInServiceInstances Auto Scaling group attribute to publish the queue messages for each instance. Create a CloudWatch subscription filter for the application logs with the Lambda function as the target. Create a target tracking scaling policy for the Auto Scaling group that uses the custom metric to scale in and out.
C. Create a target tracking scaling policy for the Auto Scaling group. In the target tracking policy, use the ApproximateNumberOfMessagesVisible SQS queue attribute and the GroupInServiceInstances Auto Scaling group attribute to calculate how many messages are in the queue for each number of instances by using metric math. Use the calculated attribute to scale in and out.
D. Create an AWS Lambda function that logs the ApproximateNumberOfMessagesVisible attribute of the SQS queue to a CloudWatch Logs log group. Schedule an Amazon EventBridge rule to run the Lambda function every 5 minutes. Create a metric filer to count the number of log events from a CloudWatch logs group. Create a target tracking scaling policy for the Auto Scaling group that uses the custom metric to scale in and out.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
A company has a single AWS account that runs hundreds of Amazon EC2 instances in a single AWS Region. The company launches and terminates new EC2 instances every hour. The account includes existing EC2 instances that have been running for longer than a week.The company's security policy requires all running EC2 instances to have an EC2 instance profile attached. The company has created a default EC2 instance profile. The default EC2 instance profile must be attached to any EC2 instances that do not have a profile attached.Which solution will meet these requirements?

A. Configure an Amazon EventBridge rule that matches the Amazon EC2 RunInstances API calls. Configure the rule to invoke an AWS Lambda function to attach the default instance profile to the EC2 instances.
B. Configure AWS Config. Deploy an AWS Config ec2-instance-profile-attached managed rule. Configure an automatic remediation action that invokes an AWS Systems Manager Automation runbook to attach the default instance profile to the EC2 instances.
C. Configure an Amazon EventBridge rule that matches the Amazon EC2 StartInstances API calls. Configure the rule to invoke an AWS Systems Manager Automation runbook to attach the default instance profile to the EC2 instances.
D. Configure AWS Config. Deploy an AWS Config iam-role-managed-policy-check managed rule. Configure an automatic remediation action that invokes an AWS Lambda function to attach the default instance profile to the EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
A company uses AWS Organizations to manage hundreds of AWS accounts. The company has a team that is responsible for AWS Identity and Access Management (IAM).The IAM team wants to implement AWS IAM Identity Center. The IAM team must have only the minimum required permissions to manage IAM Identity Center. The IAM team must not be able to gain unnecessary access to the Organizations management account. The IAM team must be able to provision new IAM Identity Center permission sets and assignments for new and existing member accounts.Which combination of steps will meet these requirements? (Choose three.)

A. Create a new AWS account for the IAM team. Enable IAM Identity Center in the new account. In the Organizations management account, register the new account as a delegated administrator for IAM Identity Center.
B. Create a new AWS account for the IAM team. Enable IAM Identity Center in the Organizations management account. In the Organizations management account, register the new account as a delegated administrator for IAM Identity Center.
C. Create an SCP in Organizations. Create a new OU for the Organizations management account, and link the new SCP to the O
D. Create IAM users and an IAM group for the IAM team in IAM Identity Center. Add the users to the group. Create a new permission set. Attach the AWSSSOMemberAccountAdministrator managed IAM policy to the group.
E. Assign the new permission set to the Organizations management account. Allow the IAM team's group to use the permission set.
F. Assign the new permission set to the new AWS account. Allow the IAM team's group to use the permission set.

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
A company uses an Amazon Aurora PostgreSQL global database that has two secondary AWS Regions. A DevOps engineer has configured the database parameter group to guarantee an RPO of 60 seconds. Write operations on the primary cluster are occasionally blocked because of the RPO setting.The DevOps engineer needs to reduce the frequency of blocked write operations.Which solution will meet these requirements?

A. Add an additional secondary cluster to the global database.
B. Enable write forwarding for the global database.
C. Remove one of the secondary clusters from the global database.
D. Configure synchronous replication for the global database.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
A company has a web application that is hosted on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster runs on AWS Fargate that is available through an internet-facing Application Load Balancer.The application is experiencing stability issues that lead to longer response times. A DevOps engineer needs to configure observability in Amazon CloudWatch to troubleshoot the issue. The solution must provide only the minimum necessary permissions.Which combination of steps will meet these requirements? (Choose three.)

A. Deploy the CloudWatch agent as a Kubernetes StatefulSet to the EKS cluster.
B. Deploy the AWS Distro for OpenTelemetry Collector as a Kubernetes DaemonSet to the EKS cluster.
C. Associate a Kubernetes service account with an IAM role by using IAM roles for service accounts in Amazon EK
D. Associate a Kubernetes service account with an IAM role by using IAM roles for service accounts in Amazon EK
E. Configure an IAM OpenID Connect (OIDC) provider for the EKS cluster.
F. Enable EKS control plane logging for the EKS cluster.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
A company stores its Python-based application code in AWS CodeCommit. The company uses AWS CodePipeline to deploy the application. The CodeCommit repository and the CodePipeline pipeline are deployed to the same AWS account.The company's security team requires all code to be scanned for vulnerabilities before the code is deployed to production. If any vulnerabilities are found, the deployment must stop.Which solution will meet these requirements?

A. Create a new CodeBuild project. Configure the project to run a security scan on the code by using Amazon CodeGuru Security. Configure the CodeBuild project to raise an error if CodeGuru Security finds vulnerabilities. Create a new IAM role that has sufficient permissions to run CodeGuru Security scans. Assign the role to the CodeBuild project. In the CodePipeline pipeline, add a new stage before the deployment stage. Select AWS CodeBuild as the action provider for the new stage. Use the source artifact from the CodeCommit repository. Configure the action to use the CodeBuild project.
B. Create a new CodeBuild project. Configure the project to run a security scan on the code by using Amazon Inspector. Configure the CodeBuild project to raise an error if Amazon Inspector finds vulnerabilities. Create a new IAM role that has sufficient permissions to run Amazon Inspector scans. Assign the role to the CodeBuild project. In the CodePipeline pipeline, add a new stage before the deployment stage. Select AWS CodeBuild as the action provider for the new stage. Use the source artifact from the CodeCommit repository. Configure the action to use the CodeBuild project.
C. Update the IAM role that is attached to CodePipeline to include sufficient permissions to invoke Amazon DevOps Guru. In the CodePipeline pipeline, add a new stage before the deployment stage. Select DevOps Guru as the action provider for the new stage. Use the source artifact from the CodeCommit repository.
D. Update the IAM role that is attached to CodePipeline to include sufficient permissions to invoke Amazon DevOps Guru. In the CodePipeline pipeline, add a new stage before the deployment stage. Select CodeGuru Security as the action provider for the new stage. Use the source artifact from the CodeCommit repository.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
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 instance 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
A company has multiple accounts in an organization in AWS Organizations. The company's SecOps team needs to receive an Amazon Simple Notification Service (Amazon SNS) notification if any account in the organization turns off the Block Public Access feature on an Amazon S3 bucket. A DevOps engineer must implement this change without affecting the operation of any AWS accounts. The implementation must ensure that individual member accounts in the organization cannot turn off the notification.Which solution will meet these requirements?

A. Designate an account to be the delegated Amazon GuardDuty administrator account. Turn on GuardDuty for all accounts across the organization. In the GuardDuty administrator account, create an SNS topic. Subscribe the SecOps team's email address to the SNS topic. In the same account, create an Amazon EventBridge rule that uses an event pattern for GuardDuty findings and a target of the SNS topic.
B. Create an AWS CloudFormation template that creates an SNS topic and subscribes the SecOps teamâ €™s email address to the SNS topic. In the template, include an Amazon EventBridge rule that uses an event pattern of CloudTrail activity for s3:PutBucketPublicAccessBlock and a target of the SNS topic. Deploy the stack to every account in the organization by using CloudFormation StackSets.
C. Turn on AWS Config across the organization. In the delegated administrator account, create an SNS topic. Subscribe the SecOps team's email address to the SNS topic. Deploy a conformance pack that uses the s3-bucket-level-public-access-prohibited AWS Config managed rule in each account and uses an AWS Systems Manager document to publish an event to the SNS topic to notify the SecOps team.
D. Turn on Amazon Inspector across the organization. In the Amazon Inspector delegated administrator account, create an SNS topic. Subscribe the SecOps teamâ€™s email address to the SNS topic. In the same account, create an Amazon EventBridge rule that uses an event pattern for public network exposure of the S3 bucket and publishes an event to the SNS topic to notify the SecOps team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
A DevOps engineer deploys an application to a fleet of Amazon Linux EC2 instances. The DevOps engineer needs to monitor system metrics across the fleet. The DevOps engineer wants to monitor the relationship between network traffic and memory utilization for the application code. The DevOps engineer wants to track the data on a 60 second interval.Which solution will meet these requirements?

A. Use Amazon CloudWatch basic monitoring to collect the NetworkIn metric and the MemoryBytesUsed metric. Graph the metrics in CloudWatch.
B. Use Amazon CloudWatch detailed monitoring to collect the NetworkIn metric and the MemoryBytesUsed metric. Graph the metrics in CloudWatch.
C. Use Amazon CloudWatch detailed monitoring to collect the NetworkIn metric. Install the CloudWatch agent on the EC2 instances to collect the mem_used metric. Graph the metrics in CloudWatch.
D. Use Amazon CloudWatch basic monitoring to collect the built-in NetworkIn metric. Install the CloudWatch agent on the EC2 instances to collect the mem_used metric. Graph the metrics in CloudWatch.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
A company uses AWS Systems Manager to manage a fleet of Amazon Linux EC2 instances that have SSM Agent installed. All EC2 instances are configured to use Instance Metadata Service Version 2 (IMDSv2) and are running in the same AWS account and AWS Region. Company policy requires developers to use only Amazon Linux.The company wants to ensure that all new EC2 instances are automatically managed by Systems Manager after creation.Which solution will meet these requirements with the MOST operational efficiency?

A. Create an IAM role that has a trust policy that allows Systems Manager to assume the role. Attach the AmazonSSMManagedEC2InstanceDefaultPolicy policy to the role. Configure the default-ec2-instance-management-role SSM service setting to use the role.
B. Ensure that AWS Config is set up. Create an AWS Config rule that validates if an EC2 instance has SSM Agent installed. Configure the rule to run on EC2 configuration changes. Configure automatic remediation for the rule to run the AWS-InstallSSMAgent SSM document to install SSM Agent.
C. Configure Systems Manager Patch Manager. Create a patch baseline that automatically installs SSM Agent on all new EC2 instances. Create a patch group for all EC2 instances. Attach the patch baseline to the patch group. Create a maintenance window and maintenance window task to start installing SSM Agent daily.
D. Create an EC2 instance role that has a trust policy that allows Amazon EC2 to assume the role. Attach the AmazonSSMManagedInstanceCore policy to the role. Ensure that AWS Config is set up. Use the ec2-instance-profile-attached managed AWS Config rule to validate if an EC2 instance has the role attached. Configure the rule to run on EC2 configuration changes. Configure automatic remediation for the rule to run the AWS-SetupManagedRoleOnEc2Instance SSM document to attach the role to the EC2 instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
A company configured an Amazon S3 event source for an AWS Lambda function. The company needs the Lambda function to run when a new object is created or an existing object is modified in a specific S3 bucket. The Lambda function will use the S3 bucket name and the S3 object key of the incoming event to read the contents of the new or modified S3 object. The Lambda function will parse the contents and save the parsed contents to an Amazon DynamoDB table.The Lambda function's execution role has permissions to read from the S3 bucket and to write to the DynamoDB table. During testing, a DevOps engineer discovers that the Lambda function does not run when objects are added to the S3 bucket or when existing objects are modified.Which solution will resolve these problems?

A. Create an S3 bucket policy for the S3 bucket that grants the S3 bucket permission to invoke the Lambda function.
B. Create a resource policy for the Lambda function to grant Amazon S3 permission to invoke the Lambda function on the S3 bucket.
C. Configure an Amazon Simple Queue Service (Amazon SQS) queue as an OnFailure destination for the Lambda function. Update the Lambda function to process messages from the SQS queue and the S3 event notifications.
D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the destination for the S3 bucket event notifications. Update the Lambda function's execution role to have permission to read from the SQS queue. Update the Lambda function to consume messages from the SQS queue.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
A company recently configured AWS Control Tower in its organization in AWS Organizations. The company enrolled all existing AWS accounts in AWS Control Tower. The company wants to ensure that all new AWS accounts are automatically enrolled in AWS Control Tower.The company has an existing AWS Step Functions workflow that creates new AWS accounts and performs any actions required as part of account creation. The Step Functions workflow is defined in the same AWS account as AWS Control Tower.Which combination of steps should the company add to the Step Functions workflow to meet these requirements? (Choose two.)

A. Create an Amazon EventBridge event that has an aws.controltower source and a CreateManagedAccount detail-type. Add the details of the new AWS account to the detail field of the event.
B. Create an Amazon EventBridge event that has an aws.controltower source and a SetupLandingZone detail-type. Add the details of the new AWS account to the detail field of the event.
C. Create an AWSControlTowerExecution role in the new AWS account. Configure the role to allow the AWS Control Tower administrator account to assume the role.
D. Call the AWS Service Catalog ProvisionProduct API operation with the details of the new AWS account.
E. Call the Organizations EnableAWSServiceAccess API operation with the controltower.amazonaws.com service name and the details of the new AWS account.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229

A company's web application uses an Application Load Balancer (ALB) to direct traffic to Amazon EC2 instances across three Availability Zones.The company has deployed a newer version of the application to one Availability Zone for testing. If a problem is detected with the application, the company wants to direct traffic away from the affected Availability Zone until the deployment has been rolled back. The application must remain available and maintain static stability during the rollback.Which solution will meet these requirements with the MOST operational efficiency?

A. Disable cross-zone load balancing on the ALB's target group. Initiate a zonal shift on the ALB to direct traffic away from the affected Availability Zone.
B. Disable cross-zone load balancing on the ALB's target group. Manually remove instances in the target group that belong to the affected Availability Zone.
C. Configure cross-zone load balancing on the ALB's target group to inherit settings from the AL
D. Configure cross-zone load balancing on the ALB's target group to inherit settings from the AL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
A company has several AWS accounts. An Amazon Connect instance runs in each account. The company uses an Amazon EventBridge default event bus in each account for event handling.A DevOps team needs to receive all the Amazon Connect events in a single DevOps account.Which solution meets these requirements?

A. Update the resource-based policy of the default event bus in each account to allow the DevOps account to replay events. Configure an EventBridge rule in the DevOps account that matches Amazon Connect events and has a target of the default event bus in the other accounts.
B. Update the resource-based policy of the default event bus in each account to allow the DevOps account to receive events. Configure an EventBridge rule in the DevOps account that matches Amazon Connect events and has a target of the default event bus in the other accounts.
C. Update the resource-based policy of the default event bus in the DevOps account. Update the policy to allow events to be received from the accounts. Configure an EventBridge rule in each account that matches Amazon Connect events and has a target of the DevOps account's default event bus.
D. Update the resource-based policy of the default event bus in the DevOps account. Update the policy to allow events to be replayed by the accounts. Configure an EventBridge rule in each account that matches Amazon Connect events and has a target of the DevOps account's default event bus.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
A company has deployed an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 node groups. The company's DevOps team uses the Kubernetes Horizontal Pod Autoscaler and recently installed a supported EKS cluster Autoscaler.The DevOps team needs to implement a solution to collect metrics and logs of the EKS cluster to establish a baseline for performance. The DevOps team will create an initial set of thresholds for specific metrics and will update the thresholds over time as the cluster is used. The DevOps team must receive an Amazon Simple Notification Service (Amazon SNS) email notification if the initial set of thresholds is exceeded or if the EKS cluster Autoscaler is not functioning properly.The solution must collect cluster, node, and pod metrics. The solution also must capture logs in Amazon CloudWatch.Which combination of steps should the DevOps team take to meet these requirements? (Choose three.)

A. Deploy the CloudWatch agent and Fluent Bit to the cluster. Ensure that the EKS cluster has appropriate permissions to send metrics and logs to CloudWatch.
B. Deploy AWS Distro for OpenTelemetry to the cluster. Ensure that the EKS cluster has appropriate permissions to send metrics and logs to CloudWatch.
C. Create CloudWatch alarms to monitor the CPU, memory, and node failure metrics of the cluster. Configure the alarms to send an SNS email notification to the DevOps team if thresholds are exceeded.
D. Create a CloudWatch composite alarm to monitor a metric log filter of the CPU, memory, and node metrics of the cluster. Configure the alarm to send an SNS email notification to the DevOps team when anomalies are detected.
E. Create a CloudWatch alarm to monitor the logs of the Autoscaler deployments for errors. Configure the alarm to send an SNS email notification to the DevOps team if thresholds are exceeded.
F. Create a CloudWatch alarm to monitor a metric log filter of the Autoscaler deployments for errors. Configure the alarm to send an SNS email notification to the DevOps team if thresholds are exceeded.

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
A company discovers that its production environment and disaster recovery (DR) environment are deployed to the same AWS Region. All the production applications run on Amazon EC2 instances and are deployed by AWS CloudFormation. The applications use an Amazon FSx for NetApp ONTAP volume for application storage. No application data resides on the EC2 instances.A DevOps engineer copies the required AMIs to a new DR Region. The DevOps engineer also updates the CloudFormation code to accept a Region as a parameter. The storage needs to have an RPO of 10 minutes in the DR Region.Which solution will meet these requirements?

A. Create an Amazon S3 bucket in both Regions. Configure S3 Cross-Region Replication (CRR) for the S3 buckets. Create a scheduled AWS Lambda function to copy any new content from the FSx for ONTAP volume to the S3 bucket in the production Region.
B. Use AWS Backup to create a backup vault and a custom backup plan that has a 10-minute frequency. Specify the DR Region as the target Region. Assign the EC2 instances in the production Region to the backup plan.
C. Create an AWS Lambda function to create snapshots of the instance store volumes that are attached to the EC2 instances. Configure the Lambda function to copy the snapshots to the DR Region and to remove the previous copies. Create an Amazon EventBridge scheduled rule that invokes the Lambda function every 10 minutes.
D. Create an FSx for ONTAP instance in the DR Region. Configure a 5-minute schedule for a volume-level NetApp SnapMirror to replicate the volume from the production Region to the DR Region.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
During a security audit, a company discovered that some security groups allow SSH traffic from 0.0.0.0/0. A security team must implement a solution to detect and remediate this issue as soon as possible. The company uses one organization in AWS Organizations to manage all the company's AWS accounts.Which solution will meet these requirements?

A. Enable AWS Config for all AWS accounts. Use a periodic trigger to activate the vpe-sg-port-restriction-check AWS Config rule. Create an AWS Lambda function to remediate any noncompliant rules.
B. Create an AWS Lambda function in each AWS account to delete all the security group rules. Create an Amazon EventBridge rule to match security group update events or creation events. Set the Lambda function in each account as a target for the rule.
C. Enable AWS Config for all AWS accounts. Create a custom AWS Config rule to run on the restricted-ssh configuration change trigger. Configure the rule to invoke an AWS Lambda function to remediate any noncompliant resources.
D. Create an AWS Systems Manager Automation document in each account to inspect all security groups and to delete noncompliant rules. Use an Amazon EventBridge rule to run the Automation document every hour.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
A company's DevOps engineer must install a software package on 30 on-premises VMs and 15 Amazon EC2 instances.The DevOps engineer needs to ensure that all VMs receive the package in a process that is auditable and that any configuration drift on the VMs is automatically identified and alerted on. The company uses AWS Direct Connect to connect its on-premises data center to AWS.Which solution will meet these requirements with the MOST operational efficiency?

A. Write a script that iterates through the list of VMs once a week. Configure the script to check for the package and install the package if the package is not found. Configure the script to send an email message notification to the system administrator if the package is not found.
B. Install the AWS Systems Manager Agent (SSM Agent) on all VMs. Use the SSM Agent to install the package. Use AWS Config to monitor for configuration drift. Use Amazon Simple Notification Service (Amazon SNS) to notify the system administrator if any drift is found.
C. Write a script that checks if the package is installed across the environment. Configure the script to create a list of all VMs that are noncompliant. Configure the script to send the list to the system administrator, who will install the package on the noncompliant VMs.
D. Log in to each V

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
A company has migrated its container-based applications to Amazon EKS and want to establish automated email notifications. The notifications sent to each email address are for specific activities related to EKS components. The solution will include Amazon SNS topics and an AWS Lambda function to evaluate incoming log events and publish messages to the correct SNS topic.Which logging solution will support these requirements?

A. Enable Amazon CloudWatch Logs to log the EKS components. Create a CloudWatch subscription filter for each component with Lambda as the subscription feed destination.
B. Enable Amazon CloudWatch Logs to log the EKS components. Create CloudWatch Logs Insights queries linked to Amazon EventBridge events that invoke Lambda.
C. Enable Amazon S3 logging for the EKS components. Configure an Amazon CloudWatch subscription filter for each component with Lambda as the subscription feed destination.

D. Enable Amazon S3 logging for the EKS components. Configure S3 PUT Object event notifications with AWS Lambda as the destination.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
A company has an AWS CodePipeline pipeline in the eu-west-1 Region. The pipeline stores the build artifacts in an Amazon S3 bucket. The pipeline builds and deploys an AWS Lambda function by using an AWS CloudFormation deploy action.A DevOps engineer needs to update the existing pipeline to also deploy the Lambda function to the us-east-1 Region. The pipeline has already been updated to create an additional artifact to deploy to us-east-1.Which combination of steps should the DevOps engineer take to meet these requirements? (Choose two.)

A. Modify the CloudFormation template to include a parameter for the Lambda function code's .zip file location. Create a new CloudFormation deploy action for us-east-1 in the pipeline. Configure the new deploy action to pass in the us-east-1 artifact location as a parameter override.
B. Create a new CloudFormation deploy action for us-east-1 in the pipeline. Configure the new deploy action to use the CloudFormation template from the additional artifact that was created for us-east-1.
C. Create an S3 bucket in us-east-1. Configure the S3 bucket policy to allow CodePipeline to have read and write access.
D. Create an S3 bucket in us-east-1. Configure S3 Cross-Region Replication (CRR) from the S3 bucket in eu-west-1 to the S3 bucket in us-east-1.
E. Modify the pipeline to include the S3 bucket for us-east-1 as an artifact store. Create a new CloudFormation deploy action for us-east-1 in the pipeline. Configure the new deploy action to use the CloudFormation template from the us-east-1 artifact.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
A company uses an AWS Cloud Development Kit (AWS CDK) application for its infrastructure. The AWS CDK application creates AWS Lambda functions and the IAM roles that are attached to the functions. The company also uses AWS Organizations. The company's developers can assume the AWS CDK application deployment role.The company's security team discovered that the developers and the role used to deploy the AWS CDK application have more permissions than necessary. The security team also discovered that the roles attached to the Lambda functions that the CDK application creates have more permissions than necessary. The developers must not have the ability to grant additional permissions.Which solution will meet these requirements with the LEAST operational overhead?

A. Create an SCP that denies the iam:CreateRole action and the iam:UpdateRole action for the developer role and the AWS CDK application deployment role. Centrally create new IAM roles to attach to the Lambda functions for the developers to use to provision Lambda functions.
B. Create an IAM permission boundary policy. Define the maximum actions that the AWS CDK application requires in the policy. Update the account's AWS CDK bootstrapping to use the permission boundary. Update the configuration in the AWS CDK application for the default permissions boundary to use the policy.
C. Create an IAM permission boundary policy. Define the maximum actions that the AWS CDK application requires in the policy. Instruct the developers to use the permission boundary policy name when they create

a role in the AWS CDK application code.

D. Create an SCP that denies the iam:CreateRole action and the iam:UpdateRole action for the developer role. Give the AWS CDK deployment role access to create roles associated with Lambda functions. Run AWS Identity and Access Management Access Analyzer to verify that the Lambda functions role does not have permissions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
A company uses Amazon Elastic Container Registry (Amazon ECR) private registries to store container images.A DevOps team needs to ensure that the container images are regularly scanned for software package vulnerabilities.Which solution will meet this requirement?

A. Enable enhanced scanning for private registries in Amazon EC
B. Enable basic continuous scanning for private registries in Amazon EC
C. Create an AWS System Manager Automation document to scan images by using the AWS SD
D. Create an AWS Lambda function that scans all images in Amazon ECR by using the AWS SD

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
A security team sets up a workflow that invokes an AWS Step Functions workflow when Amazon EventBridge matches specific events. The events can be generated by several AWS services. AWS CloudTrail records user activities.The security team notices that some important events do not invoke the workflow as expected. The CloudTrail logs do not indicate any direct errors related to the missing events.Which combination of steps will identify the root cause of the missing event invocations? (Choose three.)

A. Enable EventBridge schema discovery on the event bus to determine whether the event patterns match the expected schema.
B. Configure Amazon CloudWatch to monitor EventBridge metrics and Step Functions metrics. Set up alerts for anomalies in event patterns and workflow invocations.
C. Configure an AWS Lambda logging function to monitor and log events from EventBridge to provide more details about the processed events.
D. Review the Step Functions execution history for patterns of failures or timeouts that could correlate to the missing event invocations.
E. Review metrics for the EventBridge failed invocations to ensure that the IAM execution role that is attached to the rule has sufficient permissions.
F. Verify that the Step Functions workflow has the correct permissions to be invoked by EventBridge.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
A company's DevOps engineer uses AWS Systems Manager to perform maintenance tasks. The company has a few Amazon EC2 instances that require a restart after notifications from AWS Health.The DevOps engineer must implement an automated solution that uses Amazon EventBridge to remediate the notifications during the company's scheduled maintenance windows.How should the DevOps engineer configure an EventBridge rule to meet these requirements?

A. Configure an event source of AWS Health. Configure event types that indicate scheduled instance termination and retirement. Target the AWS-RestartEC2Instance Systems Manager Automation runbook to restart the EC2 instances.
B. Configure an event source of Systems Manager. Configure an event type that indicates a maintenance window. Target the AWS-RestartEC2Instance Systems Manager Automation runbook to restart the EC2 instances.
C. Configure an event source of AWS Health. Configure event types that indicate scheduled instance termination and retirement. Target a newly created AWS Lambda function that registers a Systems Manager maintenance window task to restart the EC2 instances.
D. Configure an event source of EC2. Configure an event type that indicates instance state notification. Target a newly created AWS Lambda function that registers a Systems Manager maintenance window task to restart the EC2 instances.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
A DevOps engineer manages an AWS CodePipeline pipeline that builds and deploys a web application on AWS. The pipeline has a source stage, a build stage, and a deploy stage. When deployed properly, the web application responds with a 200 OK HTTP response code when the URL of the home page is requested.The home page recently returned a 503 HTTP response code after CodePipeline deployed the application. The DevOps engineer needs to add an automated test into the pipeline. The automated test must ensure that the application returns a 200 OK HTTP response code after the application is deployed. The pipeline must fail if the response code is not present during the test. The DevOps engineer has added a CheckURL stage after the deploy stage in the pipeline.What should the DevOps engineer do next to implement the automated test?

A. Configure the CheckURL stage to use an Amazon CloudWatch action. Configure the action to use a canary synthetic monitoring check on the application URL and to report a success or failure to CodePipeline.
B. Create an AWS Lambda function to check the response code status of the URL and to report a success or failure to CodePipeline. Configure an action in the CheckURL stage to invoke the Lambda function.
C. Configure the CheckURL stage to use an AWS CodeDeploy action. Configure the action with an input artifact that is the URL of the application and to report a success or failure to CodePipeline.
D. Deploy an Amazon API Gateway HTTP API that checks the response code status of the URL and that reports success or failure to CodePipeline. Configure the CheckURL stage to use the AWS Device Farm test action and to provide the API Gateway HTTP API as an input artifact.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
A company has an application that uploads access logs to an Amazon CloudWatch Logs log group. The fields in the log lines include the response code and the application name.The company wants to create a

CloudWatch metric to track the number of requests by response code in a specific range and with a specific application name.Which solution will meet these requirements?

A. Create a CloudWatch Logs log event filter on the CloudWatch Logs log stream to match the response code range. Configure the log event filter to increment a metric. Set the response code and application name as dimensions.
B. Create a CloudWatch Logs metric filter on the CloudWatch Logs log group to match the response code range. Configure the metric filter to increment a metric. Set the response code and application name as dimensions.
C. Create a CloudWatch Contributor Insights rule on the CloudWatch Logs log stream with a filter to match the response code range. Configure the Contributor Insights rule to increment a CloudWatch metric with the response code and application name as dimensions.
D. Create a CloudWatch Logs Insights query on the CloudWatch Logs log group to match the response code range. Configure the Logs Insights query to increment a CloudWatch metric with the response code and application name as dimensions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
A DevOps engineer provisioned an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with managed node groups. The DevOps engineer associated an OpenID Connect (OIDC) issuer with the cluster.The DevOps engineer is configuring Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp3) volumes for the cluster. The DevOps engineer attempts to initiate a PersistentVolumeClaim (PVC) request but is unable to provision a volume. To troubleshoot the issue, the DevOps engineer runs the kubectl describe pyc command. The DevOps engineer receives a failed to provision volume with StorageClass error and a could not create volume in EC2:UnauthorizedOperation error.Which solution will resolve these errors?

A. Create a Kubernetes cluster role that allows the persistent volumes to perform get, list, watch, create, and delete operations. Configure the cluster role to allow get, list, and watch operations for storage in the cluster.
B. Create an Amazon EBS Container Storage Interface (CSI) driver IAM role that has the required permissions and trust relationships. Attach the IAM role to the Amazon EBS CSI driver add-on in the cluster.
C. Add the ebs.csi.aws.com/volumeType:gp3 annotation to the PersistentVolumeClaim object in the cluster.
D. Create a Kubernetes storage class object. Set the provisioner value to ebs.csi.aws.com. Set the volumeBindingMode value to WaitForFirstConsumer in the luster.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
A company runs a fleet of Amazon EC2 instances in a VPC. The company's employees remotely access the EC2 instances by using the Remote Desktop Protocol (RDP).The company wants to collect metrics about how many RDP sessions the employees initiate every day.Which combination of steps will meet this requirement? (Choose three.)

A. Create an Amazon EventBridge rule that reacts to EC2 Instance State-change Notification events.
B. Create an Amazon CloudWatch Logs log group. Specify the log group as a target for the EventBridge rule.

C. Create a flow log in VPC Flow Logs.
D. Create an Amazon CloudWatch Logs log group. Specify the log group as a destination for the flow log.
E. Create a log group metric filter.
F. Create a log group subscription filter. Use EventBridge as the destination.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
A company is using Amazon Elastic Kubernetes Service (Amazon EKS) to run its applications. The EKS cluster is successfully running multiple pods. The company stores the pod images in Amazon Elastic Container Registry (Amazon ECR).The company needs to configure Pod Identity access for the EKS cluster. The company has already updated the node IAM role by using the permissions for Pod Identity access.Which solution will meet these requirements?

A. Create an IAM OpenID Connect (OIDC) provider for the EKS cluster.
B. Ensure that the nodes can reach the EKS Auth AP
C. Create an EKS access entry that uses the API_AND-CONFIG_MAP cluster authentication mode.
D. Configure the AWS Security Token Service (AWS STS) endpoint for the Kubernetes service account that the pods in the EKS cluster use.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
A company is implementing an Amazon Elastic Container Service (Amazon ECS) cluster to run its workload. The company architecture will run multiple ECS services on the cluster. The architecture includes an Application Load Balancer on the front end and uses multiple target groups to route traffic.A DevOps engineer must collect application and access logs. The DevOps engineer then needs to send the logs to an Amazon S3 bucket for near-real-time analysis.Which combination of steps must the DevOps engineer take to meet these requirements? (Choose three.)

A. Download the Amazon CloudWatch Logs container instance from AW
B. Install the Amazon CloudWatch Logs agent on the ECS instances. Change the logging driver in the ECS task definition to awslogs.
C. Use Amazon EventBridge to schedule an AWS Lambda function that will run every 60 seconds and will run the Amazon CloudWatch Logs create-export-task command. Then point the output to the logging S3 bucket.
D. Activate access logging on the AL
E. Activate access logging on the target groups that the ECS services use. Then send the logs directly to the logging S3 bucket.
F. Create an Amazon Kinesis Data Firehose delivery stream that has a destination of the logging S3 bucket. Then create an Amazon CloudWatch Logs subscription filter for Kinesis Data Firehose.

Correct Answer: BDBF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
A company has multiple AWS accounts in an organization in AWS Organizations that has all features enabled. The companyâ€™s DevOps administrator needs to improve security across all the company's AWS accounts. The administrator needs to identify the top users and roles in use across all accounts.Which solution will meet these requirements with the MOST operational efficiency?

A. Create a new organization trail in AWS CloudTrail. Configure the trail to send log events to Amazon CloudWatch Logs. Create a CloudWatch Contributor Insights rule for the userIdentity.arn log field. View the results in CloudWatch Contributor Insights.
B. Create an unused access analysis for the organization by using AWS Identity and Access Management Access Analyzer. Review the analyzer results and determine if each finding has the intended level of permissions required for the workload.
C. Create a new organization trail in AWS CloudTrail. Create a table in Amazon Athena that uses partition projection. Load the Athena table with CloudTrail data. Query the Athena table to find the top users and roles.
D. Generate a Service access report for each account by using Organizations. From the results, pull the last accessed date and last accessed by account fields to find the top users and roles.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
A company has an organization in AWS Organizations with many Oils that contain many AWS accounts. The organization has a dedicated delegated administrator AWS account.The company needs the accounts in one OU to have server-side encryption enforced for all Amazon Elastic Block Store (Amazon EBS) volumes and Amazon Simple Queue Service (Amazon SQS) queues that are created or updated on an AWS CloudFormation stack.Which solution will enforce this policy before a CloudFormation stack operation in the accounts of this OU?

A. Activate trusted access to CloudFormation StackSets. Create a CloudFormation Hook that enforces server-side encryption on EBS volumes and SQS queues. Deploy the Hook across the accounts in the OU by using StackSets.
B. Set up AWS Config in all the accounts in the O
C. Write an SCP to deny the creation of EBS volumes and SQS queues unless the EBS volumes and SQS queues have server-side encryption. Attach the SCP to the O
D. Create an AWS Lambda function in the delegated administrator account that checks whether server-side encryption is enforced for EBS volumes and SQS queues. Create an IAM role to provide the Lambda function access to the accounts in the O

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
A company is running an internal application in an Amazon Elastic Container Service (Amazon ECS) cluster on Amazon EC2. The ECS cluster instances can connect to the public internet. The ECS tasks that run on the cluster instances are configured to use images from both private Amazon Elastic Container Registry (Amazon

ECR) repositories and a public ECR registry repository.A new security policy requires the company to remove the ECS cluster's direct access to the internet. The company must remove any NAT gateways and internet gateways from the VPC that hosts the cluster. A DevOps engineer needs to ensure the ECS cluster can still download images from both the public ECR registry and the private ECR repositories. Images from the public ECR registry must remain up-to-date. New versions of the images must be available to the ECS cluster within 24 hours of publication.Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

A. Create an AWS CodeBuild project and a new private ECR repository for each image that is downloaded from the public ECR registry. Configure each project to pull the image from the public ECR repository and push the image to the new private ECR repository. Create an Amazon EventBridge rule that invokes the CodeBuild project once every 24 hours. Update each task definition in the ECS cluster to refer to the new private ECR repository.
B. Create a new Amazon ECR pull through cache rule for each image that is downloaded from the public ECR registry. Create an AWS Lambda function that invokes each pull through cache rule. Create an Amazon EventBridge rule that invokes the Lambda function once every 24 hours. Update each task definition in the ECS cluster to refer to the image from the pull through cache.
C. Create a new Amazon ECR pull through cache rule for the public ECR registry. Update each task definition in the ECS cluster to refer to the image from the pull through cache. Ensure each public image has been downloaded through the pull through cache at least once before removing internet access from the VP
D. Create an Amazon ECR interface VPC endpoint for the public ECR repositories that are in the VP
E. Create an Amazon ECR interface VPC endpoint for the private ECR repositories that are in the VP
F. Create an Amazon S3 gateway endpoint in the VP

Correct Answer: CCECFC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
A company has a continuous integration pipeline where the company creates container images by using AWS CodeBuild. The created images are stored in Amazon Elastic Container Registry (Amazon ECR).Checking for and fixing the vulnerabilities in the images takes the company too much time. The company wants to identify the image vulnerabilities quickly and notify the security team of the vulnerabilities.Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Activate Amazon Inspector enhanced scanning for Amazon EC
B. Create an Amazon EventBridge rule for Amazon Inspector findings. Set an Amazon Simple Notification Service (Amazon SNS) topic as the rule target.
C. Activate AWS Lambda enhanced scanning for Amazon EC
D. Create a new AWS Lambda function. Invoke the new Lambda function when scan findings are detected.
E. Activate default basic scanning for Amazon ECR for all container images. Configure the default basic scanning to use continuous scanning. Set up a topic in Amazon Simple Notification Service (Amazon SNS).

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
A DevOps administrator is configuring a repository to store a company's container images. The administrator needs to configure a lifecycle rule that automatically deletes container images that have a specific tag and that are older than 15 days.Which solution will meet these requirements with the MOST operational efficiency?

A. Create a repository in Amazon Elastic Container Registry (Amazon ECR). Add a lifecycle policy to the repository to expire images that have the matching tag after 15 days.
B. Create a repository in AWS CodeArtifact. Add a repository policy to the CodeArtifact repository to expire old assets that have the matching tag after 15 days.
C. Create a bucket in Amazon S3. Add a bucket lifecycle policy to expire old objects that have the matching tag after 15 days
D. Create an EC2 Image Builder container recipe. Add a build component to expire the container that has the matching tag after 15 days.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
A company uses Amazon Redshift as its data warehouse solution. The company wants to create a dashboard to view changes to the Redshift users and the queries the users perform.Which combination of steps will meet this requirement? (Choose two.)

A. Create an Amazon CloudWatch log group. Create an AWS CloudTrail trail that writes to the CloudWatch log group.
B. Create a new Amazon S3 bucket. Configure default audit logging on the Redshift cluster. Configure the S3 bucket as the target.
C. Configure the Redshift cluster database audit logging to include user activity logs. Configure Amazon CloudWatch as the target.
D. Create an Amazon CloudWatch dashboard that has a log widget. Configure the widget to display user details from the Redshift logs.
E. Create an AWS Lambda function that uses Amazon Athena to query the Redshift logs. Create an Amazon CloudWatch dashboard that has a custom widget type that uses the Lambda function.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
A company uses an organization in AWS Organizations to manage its 500 AWS accounts. The organization has all features enabled. The AWS accounts are in a single OU. The developers need to use the CostCenter tag key for all resources in the organization's member accounts. Some teams do not use the CostCenter tag key to tag their Amazon EC2 instances.The cloud team wrote a script that scans all EC2 instances in the organization's member accounts. If the EC2 instances do not have a CostCenter tag key, the script will notify AWS account administrators. To avoid this notification, some developers use the CostCenter tag key with an arbitrary string in the tag value.The cloud team needs to ensure that all EC2 instances in the organization use a CostCenter tag key with the appropriate cost center value.Which solution will meet these requirements?

A. Create an SCP that prevents the creation of EC2 instances without the CostCenter tag key. Create a tag policy that requires the CostCenter tag to be values from a known list of cost centers for all EC2 instances. Attach the policy to the O
B. Create an SCP that prevents the creation of EC2 instances without the CostCenter tag key. Attach the policy to the O
C. Create an SCP that prevents the creation of EC2 instances without the CostCenter tag key. Attach the

policy to the O

D. Create a tag policy that requires the CostCenter tag to be values from a known list of cost centers for all EC2 instances. Attach the policy to the O

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
A DevOps engineer uses a pipeline in AWS CodePipeline. The pipeline has a build action and a deploy action for a single-page web application that is delivered to an Amazon S3 bucket. Amazon CloudFront serves the web application. The build action creates an artifact for the web application.The DevOps engineer has created an AWS CloudFormation template that defines the S3 bucket and configures the S3 bucket to host the application. The DevOps engineer has configured a CloudFormation deploy action before the S3 action. The CloudFormation deploy action creates the S3 bucket. The DevOps engineer needs to configure the S3 deploy action to use the S3 bucket from the CloudFormation template.Which combination of steps will meet these requirements? (Choose two.)

A. Add an output named BucketName to the CloudFormation template. Set the output's value to refer to the S3 bucket from the CloudFormation template. Configure the output value to export to an AWS::SSM::Parameter resource named Stackvariables.
B. Add an output named BucketName to the CloudFormation template. Set the output's value to refer to the S3 bucket from the CloudFormation template. Set the CloudFormation action's namespace to StackVariables in the pipeline.
C. Configure the output artifacts of the CloudFormation action in the pipeline to be an AWS Systems Manager Parameter Store parameter named StackVariables. Name the artifact BucketName.
D. Configure the build artifact from the build action as the input to the CodePipeline S3 deploy action. Configure the deploy action to deploy to the S3 bucket by using the StackVariables.BucketName variable.
E. Configure the build artifact from the build action and the AWS Systems Manager parameter as the inputs to the deploy action. Configure the deploy action to deploy to the S3 bucket by using the StackVariables.BucketName variable.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
A company used a lift and shift strategy to migrate a workload to AWS. The company has an Auto Scaling group of Amazon EC2 instances. Each EC2 instance runs a web application, a database, and a Redis cache.Users are experiencing large variations in the web application's response times. Requests to the web application go to a single EC2 instance that is under significant load. The company wants to separate the application components to improve availability and performance.Which solution will meet these requirements?

A. Create a Network Load Balancer and an Auto Scaling group for the web application. Migrate the database to an Amazon Aurora Serverless database. Create an Application Load Balancer and an Auto Scaling group for the Redis cache.
B. Create an Application Load Balancer and an Auto Scaling group for the web application. Migrate the database to an Amazon Aurora database that has a Multi-AZ deployment. Create a Network Load Balancer and an Auto Scaling group in a single Availability Zone for the Redis cache.
C. Create a Network Load Balancer and an Auto Scaling group for the web application. Migrate the database to an Amazon Aurora Serverless database. Create an Amazon ElastiCache (Redis OSS) cluster for the

cache. Create a target group that has a DNS target type that contains the ElastiCache (Redis OSS) cluster hostname.

D. Create an Application Load Balancer and an Auto Scaling group for the web application. Migrate the database to an Amazon Aurora database that has a Multi-AZ deployment. Create an Amazon ElastiCache (Redis OSS) cluster for the cache.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
A company is using AWS Organizations and wants to implement a governance strategy with the following requirements:â€¢ AWS resource access is restricted to the same two Regions for all accounts.â€¢ AWS services are limited to a specific group of authorized services for all accounts.â€¢ Authentication is provided by Active Directory.â€¢ Access permissions are organized by job function and are identical in each account.Which solution will meet these requirements?

A. Establish an organizational unit (OU) with group policies in the management account to restrict Regions and authorized services. Use AWS CloudFormation StackSets to provision roles with permissions for each job function, including an IAM trust policy for IAM identity provider authentication in each account.

B. Establish a permission boundary in the management account to restrict Regions and authorized services. Use AWS CloudFormation StackSets to provision roles with permissions for each job function, including an IAM trust policy for IAM identity provider authentication in each account.

C. Establish a service control policy in the management account to restrict Regions and authorized services. Use AWS Resource Access Manager (AWS RAM) to share management account roles with permissions for each job function, including AWS IAM Identity Center for authentication in each account.

D. Establish a service control policy in the management account to restrict Regions and authorized services. Use AWS CloudFormation StackSets to provision roles with permissions for each job function, including an IAM trust policy for IAM identity provider authentication in each account.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
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. Run 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. Run the AWS-AmazonLinuxDefaultPatchBaseline document using the run command to verify and install patches.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
A company detects unusual login attempts in many of its AWS accounts. A DevOps engineer must implement a solution that sends a notification to the company's security team when multiple failed login attempts occur. The DevOps engineer has already created an Amazon Simple Notification Service (Amazon SNS) topic and has subscribed the security team to the SNS topic.Which solution will provide the notification with the LEAST operational effort?

A. Configure AWS CloudTrail to send management events to an Amazon CloudWatch Logs log group. Create a CloudWatch Logs metric filter to match failed ConsoleLogin events. Create a CloudWatch alarm that is based on the metric filter. Configure an alarm action to send messages to the SNS topic.
B. Configure AWS CloudTrail to send management events to an Amazon S3 bucket. Create an Amazon Athena query that returns a failure if the query finds failed logins in the logs in the S3 bucket. Create an Amazon EventBridge rule to periodically run the query. Create a second EventBridge rule to detect when the query fails and to send a message to the SNS topic.
C. Configure AWS CloudTrail to send data events to an Amazon CloudWatch Logs log group. Create a CloudWatch logs metric filter to match failed ConsoleLogin events. Create a CloudWatch alarm that is based on the metric filter. Configure an alarm action to send messages to the SNS topic.
D. Configure AWS CloudTrail to send data events to an Amazon S3 bucket. Configure an Amazon S3 event notification for the s3:ObjectCreated event type. Filter the event type by ConsoleLogin failed events. Configure the event notification to forward to the SNS topic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
A company has deployed a new REST API by using Amazon API Gateway. The company uses the API to access confidential data. The API must be accessed from only specific VPCs in the company.Which solution will meet these requirements?

A. Create and attach a resource policy to the API Gateway AP
B. Add a security group to the API Gateway AP
C. Create and attach an IAM role to the API Gateway AP
D. Add an ACL to the API Gateway AP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
A company runs a website by using an Amazon Elastic Container Service (Amazon ECS) service that is connected to an Application Load Balancer (ALB). The service was in a steady state with tasks responding to requests successfully.A DevOps engineer updated the task definition with a new container image and deployed the new task definition to the service. The DevOps engineer noticed that the service is frequently stopping and starting new tasks because the ALB healtth checks are failing.What should the DevOps engineer do to

troubleshoot the failed deployment?

A. Ensure that a security group associated with the service allows traffic from the AL
B.
C. Increase the service minimum healthy percent setting.
D. Decrease the ALB health check interval.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
A company that uses electronic patient health records runs a fleet of Amazon EC2 instances with an Amazon Linux operating system. The company must continuously ensure that the EC2 instances are running operating system patches and application patches that are in compliance with current privacy regulations. The company uses a custom repository to store application patches.A DevOps engineer needs to automate the deployment of operating system patches and application patches. The DevOps engineer wants to use both the default operating system patch repository and the custom patch repository.Which solution will meet these requirements with the LEAST effort?

A. Use AWS Systems Manager to create a new custom patch baseline that includes the default operating system repository and the custom repository. Run the AWS-RunPatchBaseline document by using the Run command to verify and install patches. Use the BaselineOverride API to configure the new custom patch baseline.
B. Use AWS Direct Connect to integrate the custom repository with the EC2 instances. Use Amazon EventBridge events to deploy the patches.
C. Use the yum-config-manager command to add the custom repository to the /etc/yum.repos.d configuration. Run the yum-config-manager-enable command to activate the new repository.
D. Use AWS Systems Manager to create a patch baseline for the default operating system repository and a second patch baseline for the custom repository. Run the AWS-RunPatchBaseline document by using the Run command to verify and install patches. Use the BaselineOverride API to configure the default patch baseline and the custom patch baseline.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
A company use an organization in AWS Organizations to manage multiple AWS accounts. The company has enabled all features enabled for the organization. The company configured the organization as a hierarchy of OUs under the root OU. The company recently registered all its OUs and enrolled all its AWS accounts in AWS Control Tower.The company needs to customize the AWS Control Tower managed AWS Config configuration recorder in each of the company's AWS accounts. The company needs to apply the customizations to both the existing AWS accounts and to any new AWS accounts that the company enrolls in AWS Control Tower in the future.Which combination of steps will meet these requirements? (Choose three.)

A. Create a new AWS account. Create an AWS Lambda function in the new account to apply the customizations to the AWS Config configuration recorder in each AWS account in the organization.
B. Create a new AWS account as an AWS Config delegated administrator. Create an AWS Lambda function in the delegated administrator account to apply the customizations to the AWS Config configuration recorder in the delegated administrator account.

C. Configure an Amazon EventBridge rule in the AWS Control Tower management account to invoke an AWS Lambda function when the Organizations OU is registered or reregistered. Re-register the root Organizations O
D. Configure the AWSControlTowerExecution IAM role in each AWS account in the organization to be assumable by an AWS Lambda function. Configure the Lambda function to assume the AWSControlTowerExecution IAM role.
E. Create an IAM role in the AWS Control Tower management account that an AWS Lambda function can assume. Grant the IAM role permission to assume the AWSControlTowerExecution IAM role in any account in the organization. Configure the Lambda function to use the new IAM role.
F. Configure an Amazon EventBridge rule in the AWS Control Tower management account to invoke an AWS Lambda function when an AWS account is updated or enrolled in AWS Control Tower or when the landing zone is updated. Re-register each Organizations OU in the organization.

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
A company runs an application in an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances run Docker containers that make requests to a MySQL database that runs on separate EC2 instances.A DevOps engineer needs to update the application to use a serverless architecture.Which solution will meet this requirement with the FEWEST changes?

A. Replace the containers that run on EC2 instances and the ALB with AWS Lambda functions. Replace the MySQL database with an Amazon Aurora Serverless v2 database that is compatible with MySQ
B. Replace the containers that run on EC2 instances with AWS Fargate. Replace the MySQL database with an Amazon Aurora Serverless v2 database that is compatible with MySQ
C. Replace the containers that run on EC2 instances and the ALB with AWS Lambda functions. Replace the MySQL database with Amazon DynamoDB tables.
D. Replace the containers that run on EC2 instances with AWS Fargate. Replace the MySQL database with Amazon DynamoDB tables.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
A company uses an organization in AWS Organizations to manage 10 AWS accounts. All features are enabled, and trusted access for AWS CloudFormation is enabled.A DevOps engineer needs to use CloudFormation to deploy an IAM role to the Organizations management account and all member accounts in the organization.Which solution will meet these requirements with the LEAST operational overhead?

A. Create a CloudFormation StackSet that has service-managed permissions. Set the root OU as a deployment target.
B. Create a CloudFormation StackSet that has service-managed permissions. Set the root OU as a deployment target. Deploy a separate CloudFormation stack in the Organizations management account.
C. Create a CloudFormation StackSet that has self-managed permissions. Set the root OU as a deployment target.
D. Create a CloudFormation StackSet that has self-managed permissions. Set the root OU as a deployment target. Deploy a separate CloudFormation stack in the Organizations management account.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
A company runs an application that stores artifacts in an Amazon S3 bucket. The application has a large user base. The application writes a high volume of objects to the S3 bucket. The company has enabled event notifications for the S3 bucket.When the application writes an object to the S3 bucket, several processing tasks need to be performed simultaneously. The company's DevOps team needs to create an AWS Step Functions workflow to orchestrate the processing tasks.Which combination of steps should the DevOps team take to meet these requirements with the LEAST operational overhead? (Choose two.)

A. Create a Standard workflow that contains a parallel state that defines the processing tasks. Create an Asynchronous Express workflow that contains a parallel state that defines the processing tasks.
B. Create a Synchronous Express workflow that contains a map state that defines the processing tasks.
C. Create an Amazon EventBridge rule to match when a new S3 object is created. Configure the EventBridge rule to invoke an AWS Lambda function. Configure the Lambda function to start the processing workflow.
D. Create an Amazon EventBridge rule to match when a new S3 object is created. Configure the EventBridge rule to start the processing workflow.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
A DevOps team supports an application that runs in an Amazon Elastic Container Service (Amazon ECS) cluster behind an Application Load Balancer (ALB). Currently, the DevOps team uses AWS CodeDeploy to deploy the application by using a blue/green all-at-once strategy. Recently, the DevOps team had to roll back a deployment when a new version of the application dramatically increased response times for requests.The DevOps team needs use to a deployment strategy that will allow the team to monitor a new version of the application before the team shifts all traffic to the new version. If a new version of the application increases response times, the deployment should be rolled back as quickly as possible.Which combination of steps will meet these requirements? (Choose two.)

A. Modify the CodeDeploy deployment to use the CodeDeployDefault.ECSCanary10Percent5Minutes configuration.
B. Modify the CodeDeploy deployment to use the CodeDeployDefault.ECSLinear10PercentEvery3Minutes configuration.
C. Create an Amazon CloudWatch alarm to monitor the UnHealthyHostCount metric for the AL
D. Create an Amazon CloudWatch alarm to monitor the TargetResponseTime metric for the AL
E. Create an Amazon CloudWatch alarm to monitor the TargetConnectionErrorCount metric for the AL

Correct Answer: ADB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267

A security team must record the configuration of AWS resources, detect issues, and send notifications for findings. The main workload in the AWS account consists of an Amazon EC2 Auto Scaling group that scales in and out several times during the day.The team wants to be notified within 2 days if any Amazon EC2 security group allows traffic on port 22 for 0.0.0.0/0. The team also needs a snapshot of the configuration of the AWS resources to be taken routinely.The security team has already created and subscribed to an Amazon Simple Notification Service (Amazon SNS) topic.Which solution meets these requirements?

A. Configure AWS Config to use periodic recording for the AWS account. Deploy the vpc-sg-port-restriction-check AWS Config managed rule. Configure AWS Config to use the SNS topic as the target for notifications.
B. Configure AWS Config to use configuration change recording for the AWS account. Deploy the vpc-sg-open-only-to-authorized-ports AWS Config managed rule. Configure AWS Config to use the SNS topic as the target for notifications.
C. Configure AWS Config to use configuration change recording for the AWS account. Deploy the ssh-restricted AWS Config managed rule. Configure AWS Config to use the SNS topic as the target for notifications.
D. Create an AWS Lambda function to evaluate security groups and publish a message to the SNS topic. Use an Amazon EventBridge rule to schedule the Lambda function to run once a day.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268
A company is using AWS CodePipeline to automate its release pipeline. AWS CodeDeploy is being used in the pipeline to deploy an application to Amazon Elastic Container Service (Amazon ECS) using the blue/green deployment model. The company wants to implement scripts to test the green version of the application before shifting traffic. These scripts will complete in 5 minutes or less. If errors are discovered during these tests, the application must be rolled back.Which strategy will meet these requirements?

A. Add a stage to the CodePipeline pipeline between the source and deploy stages. Use AWS CodeBuild to create a runtime environment and build commands in the buildspec file to invoke test scripts. If errors are found, use the aws deploy stop-deployment command to stop the deployment.
B. Add a stage to the CodePipeline pipeline between the source and deploy stages. Use this stage to invoke an AWS Lambda function that will run the test scripts. If errors are found, use the aws deploy stop-deployment command to stop the deployment.
C. Add a hooks section to the CodeDeploy AppSpec file. Use the AfterAllowTestTraffic lifecycle event to invoke an AWS Lambda function to run the test scripts. If errors are found, exit the Lambda function with an error to initiate rollback.
D. Add a hooks section to the CodeDeploy AppSpec file. Use the AfterAllowTraffic lifecycle event to invoke the test scripts. If errors are found, use the aws deploy stop-deployment CLI command to stop the deployment.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
A company has proprietary data available by using an Amazon CloudFront distribution. The company needs to ensure that the distribution is accessible by only users from the corporate office that have a known set of IP address ranges. An AWS WAF web ACL is associated with the distribution and has a default action set to Count.Which solution will meet these requirements with the LEAST operational overhead?

A. Create a new regex pattern set. Add the regex pattern set to a new rule group. Create a new web ACL that has a default action set to Block. Associate the web ACL with the CloudFront distribution. Add a rule that allows traffic based on the new rule group.
B. Create an AWS WAF IP address set that matches the corporate office IP address range. Create a new web ACL that has a default action set to Allow. Associate the web ACL with the CloudFront distribution. Add a rule that allows traffic from the IP address set.
C. Create a new regex pattern set. Add the regex pattern set to a new rule group. Set the default action on the existing web ACL to Allow. Add a rule that has priority 0 that allows traffic based on the regex pattern set.
D. Create a WAF IP address set that matches the corporate office IP address range. Set the default action on the existing web ACL to Block. Add a rule that has priority 0 that allows traffic from the IP address set.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
A company runs several applications in the same AWS account. The applications send logs to Amazon CloudWatch.A data analytics team needs to collect performance metrics and custom metrics from the applications. The analytics team needs to transform the metrics data before storing the data in an Amazon S3 bucket. The analytics team must automatically collect any new metrics that are added to the CloudWatch namespace.Which solution will meet these requirements with the LEAST operational overhead?

A. Configure a CloudWatch metric stream to include metrics from the application and the CloudWatch namespace. Configure the metric stream to deliver the metrics to an Amazon Data Firehose delivery stream. Configure the Firehose delivery stream to invoke an AWS Lambda function to transform the data. Configure the delivery stream to send the transformed data to the S3 bucket.
B. Configure a CloudWatch metrics stream to include all the metrics and to deliver the metrics to an Amazon Data Firehose delivery stream. Configure the Firehose delivery stream to invoke an AWS Lambda function to transform the data. Configure the delivery stream to send the transformed data to the S3 bucket.
C. Configure metric filters for the CloudWatch logs to create custom metrics. Configure a CloudWatch metric stream to deliver the application metrics to the S3 bucket.
D. Configure subscription filters on the application log groups to target an Amazon Data Firehose delivery stream. Configure the Firehose delivery stream to invoke an AWS Lambda function to transform the data. Configure the delivery stream to send the transformed data to the S3 bucket.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
A company uses an HPC platform to run analysis jobs for data. The company uses AWS CodeBuild to create container images and store the images on Amazon Elastic Container Registry (Amazon ECR). The images are then deployed on Amazon Elastic Kubernetes Service (Amazon EKS).To maintain compliance, the company needs to ensure that the images are signed before the images are deployed on Amazon EKS. The signing keys must be rotated periodically and must be managed automatically. The company needs to track who generates the signatures.Which solution will meet these requirements with the LEAST operational effort?

A. Use CodeBuild to retrieve the image that was previously pushed to Amazon EC
B. Use AWS Lambda to retrieve the image that was previously pushed to Amazon EC
C. Use AWS Lambda to retrieve the image that was previously pushed to Amazon EC

D. Use CodeBuild to build the image. Sign the image by using AWS Signer before pushing the image to Amazon EC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
A company uses an AWS CodeArtifact repository to store Python packages that the company developed internally. A DevOps engineer needs to use AWS CodeDeploy to deploy an application to an Amazon EC2 instance. The application uses a Python package that is stored in the CodeArtifact repository. A BeforeInstall lifecycle event hook will install the package.The DevOps engineer needs to grant the EC2 instance access to the CodeArtifact repository.Which solution will meet this requirement?

A. Create a service-linked role for CodeArtifact. Associate the role with the EC2 instance. Use the aws codeartifact get-authorization-token CLI command on the instance.
B. Configure a resource-based policy for the CodeArtifact repository that allows the ReadFromRepository action for the EC2 instance principal.
C. Configure ACLs on the CodeArtifact repository to allow the EC2 instance to access the Python package.
D. Create an instance profile that contains an IAM role that has access to CodeArtifact. Associate the instance profile with the EC2 instance. Use the aws codeartifact login CLI command on the instance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
A company has a file-reading application that saves files to a database that runs on Amazon EC2 instances. Regulations require the company to delete files from EC2 instances every day at a specific time. The company must delete database records that are older than 60 days.The database record deletion must occur after the file deletions. The company has created scripts to delete files and database records. The company needs to receive an email notification for any failure of the deletion scripts.Which solution will meet these requirements with the LEAST development effort?

A. Use AWS Systems Manager State Manager to automatically invoke a Systems Manager Automation document at the specified time each day. Configure the Automation document to use a run command to run the deletion scripts in sequential order. Create an Amazon EventBridge rule to use Amazon Simple Notification Service (Amazon SNS) to send failure notifications to the company.
B. Use AWS Systems Manager State Manager to automatically invoke a Systems Manager Automation document at the specified time each day. Configure the Automation document to use a run command to run the deletion scripts in sequential order. Create a conditional statement inside the Automation document as the last step to check for errors. Use Amazon Simple Email Service (Amazon SES) to send failure notifications as email messages to the company.
C. Create an Amazon EventBridge rule that invokes an AWS Lambda function at the specified time. Add the necessary permissions for the invocation to the Lambda function's resource-based policy. Configure the Lambda function to run the deletion scripts in sequential order. Configure the Lambda function to use Amazon Simple Notification Service (Amazon SNS) to send failure notifications to the company.
D. Create an Amazon EventBridge rule that invokes an AWS Lambda function at the specified time. Add the necessary permissions for the invocation to the Lambda function's resource-based policy. Configure the Lambda function to run the deletion scripts in sequential order. Configure the Lambda function to use Amazon Simple Email Service (Amazon SES) to send failure notifications as email messages to the

company.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
A company uses an organization in AWS Organizations that has all features enabled to manage its AWS accounts. Amazon EQ instances run in the AWS accounts.The company requires that all current EC2 instances must use Instance Metadata Service Version 2 (IMDSv2). The company needs to block AWS API calls that originate from EC2 instances that do not use IMDSv2.Which solution will meet these requirements?

A. Create a new SCP statement that denies the ec2:RunInstances action when the ec2:MetadataHttpTokens condition key is not equal to the value of required. Attach the SCP to the root of the organization.
B. Create a new SCP statement that denies the ec2:RunInstances action when the ec2:MetadataHttpPutResponseHopLimit condition key value is greater than two. Attach the SCP to the root of the organization.
C. Create a new SCP statement that denies "*" when the ec2:RoleDelivery condition key value is less than two. Attach the SCP to the root of the organization.
D. Create a new SCP statement that denies when the ec2:MetadataHttpTokens condition key value is not equal to required. Attach the SCP to the root of the organization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
A DevOps team supports an application that runs on a large number of Amazon EC2 instances in an Auto Scaling group. The DevOps team uses AWS CloudFormation to deploy the EC2 instances. The application recently experienced an issue. A single instance returned errors to a large percentage of requests. The EC2 instance responded as healthy to both Amazon EC2 and Elastic Load Balancing health checks.The DevOps team collects application logs in Amazon CloudWatch by using the embedded metric format. The DevOps team needs to receive an alert if any EC2 instance is responsible for more than half of all errors.Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

A. Create a CloudWatch Contributor Insights rule that groups logs from the CloudWatch application logs based on instance ID and errors.
B. Create a resource group in AWS Resource Groups. Use the CloudFormation stack to group the resources for the application. Add the application to CloudWatch Application Insights. Use the resource group to identify the application.
C. Create a metric filter for the application logs to count the occurrence of the term "Error." Create a CloudWatch alarm that uses the METRIC_COUNT function to determine whether errors have occurred. Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic to notify the DevOps team.
D. Create a CloudWatch alarm that uses the INSIGHT_RULE_METRIC function to determine whether a specific instance is responsible for more than half of all errors reported by EC2 instances. Configure the CloudWatch alarm to send a notification to an Amazon Simple Notification Service (Amazon SNS) topic to notify the DevOps team.
E. Create a CloudWatch subscription filter for the application logs that filters for errors and invokes an AWS Lambda function. Configure the Lambda function to send the instance ID and error and in a notification to an Amazon Simple Notification Service (Amazon SNS) topic to notify the DevOps team.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
A company is using AWS CloudFormation to perform deployments of its application environment. A deployment failed during a recent update to the existing CloudFormation stack. A DevOps engineer discovered that some resources in the stack were manually modified.The DevOps engineer needs a solution that detects manual modification of resources and sends an alert to the DevOps lead.Which solution will meet these requirements with the LEAST operational effort?

A. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the DevOps lead to the topic by using an email address. Create an AWS Config managed rule that has the CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK identifier. Create an Amazon EventBridge rule that is invoked on the NON_COMPLIANT resources status. Set the SNS topic as the rule target.
B. Tag all CloudFormation resources with a specific tag. Create an AWS Config custom rule by using the AWS Config Rules Development Kit Library (RDKlib) that checks all resource changes that have the specific tag. Configure the custom rule to mark all the tagged resource changes as NON_COMPLIANT when the change is not performed by CloudFormation. Create an Amazon EventBridge rule that is invoked on the NON_COMPUANT resources status. Create an AWS Lambda function that sends an email message to the DevOps lead. Set the Lambda function as the rule target.
C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the DevOps lead to the topic by using an email address. Create an AWS Config managed rule that has the CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK identifier. Create an Amazon EventBridge rule that is invoked on the COMPLIANT resources status. Set the SNS topic as the rule target.
D. Create an AWS Config managed rule that has the CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK identifier. Create an Amazon EventBridge rule that is invoked on the NON_COMPLIANT resources status. Create an AWS Lambda function that sends an email message to the DevOps lead. Set the Lambda function as the rule target.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
A DevOps engineer deployed multiple AWS accounts by using AWS Control Tower to support different business, technical, and administrative units in a company. A security team needs the DevOps engineer to automate AWS Control Tower guardrails for the company. The guardrails must be applied to all accounts in an OU of the company's organization in AWS Organizations.The security team needs a solution that has version control and can be reviewed and rolled back if necessary. The security team will maintain the management of the solution in its OU. The security team wants to limit the type of guardrails that are allowed and allow only new guardrails that are approved by the security team.Which solution will meet these requirements with the MOST operational efficiency?

A. Create individual AWS CloudFormation templates that align to a guardrail. Store the templates in an AWS CodeCommit repository. Create an AWS::ControlTower::EnableControl logical resource in the template for each OU in the organization. Configure an AWS Code Build project that an Amazon EventBridge rule will invoke for the security team's AWS CodeCommit changes.
B. Create individual AWS CloudFormation templates that align to a guardrail. Store the templates in an AWS CodeCommit repository. Create an AWS::ControlTower::EnableControl logical resource in the template for each account in the organization. Configure an AWS CodePipeline pipeline in the security team's account.

Advise the security team to invoke the pipeline and provide these parameters when starting the pipeline.

C. Create individual AWS CloudFormation templates that align to a guardrail. Store the templates in an AWS CodeCommit repository. Create an AWS::ControlTower::EnableControl logical resource in the template for each OU in the organization. Configure an AWS CodePipeline pipeline in the security team's account that an Amazon EventBridge rule will invoke for the security team's CodeCommit changes.

D. Configure an AWS CodePipeline pipeline in the security team's account that an Amazon EventBridge rule will invoke for PutObject events to an Amazon S3 bucket. Create individual AWS CloudFormation templates that align to a guardrail. Store the templates in the S3 bucket. Create an AWS::ControlTower::EnableControl logical resource in the template for each OU in the organization.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
A company runs a web application on Amazon Elastic Kubernetes Service (Amazon EKS). The company uses Amazon CloudFront to distribute the application. The company recently enabled AWS WAF. The company set up Amazon CloudWatch Logs to send logs to an aws-waf-logs log group.The company wants a DevOps engineer to receive alerts if there are sudden changes in blocked traffic. The company does not want to receive alerts for other changes in AWS WAF log behavior. The company will tune AWS WAF rules over time.The DevOps engineer is currently subscribed to an Amazon Simple Notification Service (Amazon SNS) topic in the environment.Which solution will meet these requirements?

A. Create a CloudWatch Logs metrics filter for blocked requests on the AWS WAF log group to create a custom metric. Create a CloudWatch alarm by using CloudWatch anomaly detection and the published custom metric. Configure the alarm to notify the SNS topic to alert the DevOps engineer.

B. Create a CloudWatch anomaly detector for the log group. Create a CloudWatch alarm by using metrics that the CloudWatch anomaly detector publishes. Use the high setting for the LogAnomalyPriority metric. Configure the alarm to go into alarm state if a static threshold of one anomaly is detected. Configure the alarm to notify the SNS topic to alert the DevOps engineer.

C. Create a CloudWatch metrics filter for counted requests on the AWS WAF log group to create a custom metric. Create a CloudWatch alarm that activates when the sum of blocked requests in the custom metric during a period of 1 hour is greater than a static estimate for the acceptable number of blocked requests in 1 hour. Configure the alarm to notify the SNS topic to alert the DevOps engineer.

D. Create a CloudWatch anomaly detector for the log group. Create a CloudWatch alarm by using metrics that the CloudWatch anomaly detector publishes. Use the medium setting for the LogAnomalyPriority metric. Configure the alarm to go into alarm state if a sum of anomalies over 1 hour is greater than an expected value. Configure the alarm to notify the SNS topic to alert the DevOps engineer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
A company uses AWS Storage Gateway in file gateway mode in front of an Amazon S3 bucket that is used by multiple resources. In the morning when business begins, users do not see the objects processed by a third party the previous evening. When a DevOps engineer looks directly at the S3 bucket, the data is there, but it is missing in Storage Gateway.Which solution ensures that all the updated third-party files are available in the morning?

A. Configure a nightly Amazon EventBridge event to invoke an AWS Lambda function to run the RefreshCache command for Storage Gateway.

B. Instruct the third party to put data into the S3 bucket using AWS Transfer for SFT
C. Modify Storage Gateway to run in volume gateway mode.
D. Use S3 Same-Region Replication to replicate any changes made directly in the S3 bucket to Storage Gateway.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
A video platform company is migrating its video catalog to AWS. The company will host MP4 videos files in an Amazon S3 bucket. The company will use Amazon CloudFront and Amazon EC2 instances to serve the video files.Users first connect to a frontend application that redirects to a video URL. The video URL contains an authorization token in CloudFront. The cache is activated on the CloudFront distribution. Authorization token check activity needs to be logged in Amazon CloudWatch.The company wants to prevent direct access to video files on CloudFront and Amazon S3 and wants to implement checks of the authorization token that the frontend application provides. The company also wants to perform regular rolling updates of the code that checks the authorization token signature.Which solution will meet these requirements with the LEAST operational effort?

A. Implement an authorization token check in Lambda@Edge as a trigger on the CloudFront distribution. Enable CloudWatch logging for the Lambda@Edge function. Attach the Lambda@Edge function to the CloudFront distribution. Implement CloudFront continuous deployment to perform updates.
B. Implement an authorization token check in CloudFront Functions. Enable CloudWatch logging for the CloudFront function. Attach the CloudFront function to the CloudFront distribution. Implement CloudFront continuous deployment to perform updates.
C. Implement an authorization token check in the application code that is installed on the EC2 instances. Install the CloudWatch agent on the EC2 instances. Configure the application to log to the CloudWatch agent. Implement a second CloudFront distribution. Migrate the traffic from the first CloudFront distribution by using Amazon Route 53 weighted routing.
D. Implement an authorization token check in CloudFront Functions. Enable CloudWatch logging for the CloudFront function. Attach the CloudFront function to the CloudFront distribution. Implement a second CloudFront distribution. Migrate the traffic from the first CloudFront distribution by using Amazon Route 53 weighted routing.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
A company uses an organization in AWS Organizations to manage multiple AWS accounts in a hierarchical structure. An SCP that is associated with the organization root allows IAM users to be created.A DevOps team must be able to create IAM users with any level of permissions. Developers must also be able to create IAM users. However, developers must not be able to grant new IAM users excessive permissions. The developers have the CreateAndManageUsers role in each account. The DevOps team must be able to prevent other users from creating IAM users.Which combination of steps will meet these requirements? (Choose two.)

A. Create an SCP in the organization to deny users the ability to create and modify IAM users. Attach the SCP to the root of the organization. Attach the CreateAndManageUsers role to developers.
B. Create an SCP in the organization to grant users that have the DeveloperBoundary policy attached the ability to create new IAM users and to modify IAM users. Configure the SCP to require users to attach the

PermissionBoundaries policy to any new IAM user. Attach the SCP to the root of the organization.

C. Create an IAM permissions policy named PermissionBoundaries within each account. Configure the PermissionBoundaries policy to specify the maximum permissions that a developer can grant to a new IAM user.

D. Create an IAM permissions policy named PermissionBoundaries within each account. Configure PermissionsBoundaries to allow users who have the PermissionBoundaries policy to create new IAM users.

E. Create an IAM permissions policy named DeveloperBoundary within each account. Configure the DeveloperBoundary policy to allow developers to create IAM users and to assign policies to IAM users of only if the developer includes the PermissionBoundaries policy as the permissions boundary. Attach the DeveloperBoundary policy to the CreateAndManageUsers role within each account.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
A company has deployed a landing zone that has a well-defined AWS Organizations structure and an SCP. The company's development team can create their AWS resources only by using AWS CloudFormation and the AWS Cloud Development Kit (AWS CDK).A DevOps engineer notices that Amazon Simple Queue Service (Amazon SQS) queues that are deployed in different CloudFormation stacks have different configurations. The DevOps engineer also notices that the application cost allocation tag is not always set.The DevOps engineer needs a solution that will enforce tagging and promote the reuse of code. The DevOps engineer needs to avoid different configurations for the deployed SQS queues.What should the DevOps engineer do to meet these requirements?

A. Create an Organizations tag policy to enforce the cost allocation tag in CloudFormation stacks. Instruct the development team to use CloudFormation to define SQS queues. Instruct the development team to deploy the SQS queues by using CloudFormation StackSets.

B. Update the SCP to enforce the cost allocation tag in CloudFormation stacks. Instruct the development team to use CloudFormation modules to define SQS queues. Instruct the development team to deploy the SQS queues by using CloudFormation stacks.

C. Use AWS CDK tagging to enforce the cost allocation tag in CloudFormation StackSets. Instruct the development team to use the AWS CDK to define SQS queues. Instruct the development team to deploy the SQS queues by using CDK stacks.

D. Use AWS CDK tagging to enforce the cost allocation tag in CloudFormation stacks. Instruct the development team to use the AWS CDK to define SQS queues. Instruct the development team to deploy the SQS queues by using CDK feature flags.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
A DevOps team manages a company's AWS account. The company wants to ensure that specific AWS resource configuration changes are automatically reverted.Which solution will meet this requirement?

A. Use AWS Config rules to detect changes in resource configurations. Configure remediation action that uses AWS Systems Manager Automation documents to revert the configuration changes.

B. Use Amazon CloudWatch alarms to monitor resource metrics. When an alarm is activated, use an Amazon Simple Notification Service (Amazon SNS) topic to notify an administrator to manually reverts the configuration changes.

C. Use AWS CloudFormation to create a stack that deploys the necessary configuration changes. Update the stack when configuration changes need to be reverted.
D. Use AWS Trusted Advisor to check for noncompliant configurations. Manually apply necessary changes based on Trusted Advisor recommendations.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
A DevOps engineer needs to back up sensitive Amazon S3 objects that are stored within an S3 bucket with a private bucket policy using S3 cross-Region replication functionality. The objects need to be copied to a target bucket in a different AWS Region and account.Which combination of actions should be performed to enable this replication? (Choose three.)

A. Create a replication IAM role in the source account
B. Create a replication I AM role in the target account.
C. Add statements to the source bucket policy allowing the replication IAM role to replicate objects.
D. Add statements to the target bucket policy allowing the replication IAM role to replicate objects.
E. Create a replication rule in the source bucket to enable the replication.
F. Create a replication rule in the target bucket to enable the replication.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
A company has multiple member accounts that are part of an organization in AWS Organizations. The security team needs to review every Amazon EC2 security group and their inbound and outbound rules. The security team wants to programmatically retrieve this information from the member accounts using an AWS Lambda function in the management account of the organization.Which combination of access changes will meet these requirements? (Choose three.)

A. Create a trust relationship that allows users in the member accounts to assume the management account IAM role.
B. Create a trust relationship that allows users in the management account to assume the IAM roles of the member accounts.
C. Create an IAM role in each member account that has access to the AmazonEC2ReadOnlyAccess managed policy.
D. Create an I AM role in each member account to allow the sts:AssumeRole action against the management account IAM role's AR
E. Create an I AM role in the management account that allows the sts:AssumeRole action against the member account IAM role's AR
F. Create an IAM role in the management account that has access to the AmazonEC2ReadOnlyAccess managed policy.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286
A space exploration company receives telemetry data from multiple satellites. Small packets of data are received through Amazon API Gateway and are placed directly into an Amazon Simple Queue Service (Amazon SQS) standard queue. A custom application is subscribed to the queue and transforms the data into a standard format.Because of inconsistencies in the data that the satellites produce, the application is occasionally unable to transform the data. In these cases, the messages remain in the SQS queue. A DevOps engineer must develop a solution that retains the failed messages and makes them available to scientists for review and future processing.Which solution will meet these requirements?

A. Configure AWS Lambda to poll the SQS queue and invoke a Lambda function to check whether the queue messages are valid. If validation fails, send a copy of the data that is not valid to an Amazon S3 bucket so that the scientists can review and correct the data. When the data is corrected, amend the message in the SQS queue by using a replay Lambda function with the corrected data.
B. Convert the SQS standard queue to an SQS FIFO queue. Configure AWS Lambda to poll the SQS queue every 10 minutes by using an Amazon EventBridge schedule. Invoke the Lambda function to identify any messages with a SentTimestamp value that is older than 5 minutes, push the data to the same location as the application's output location, and remove the messages from the queue.
C. Create an SQS dead-letter queue. Modify the existing queue by including a redrive policy that sets the Maximum Receives setting to 1 and sets the dead-letter queue ARN to the ARN of the newly created queue. Instruct the scientists to use the dead-letter queue to review the data that is not valid. Reprocess this data at a later time.
D. Configure API Gateway to send messages to different SQS virtual queues that are named for each of the satellites. Update the application to use a new virtual queue for any data that it cannot transform, and send the message to the new virtual queue. Instruct the scientists to use the virtual queue to review the data that is not valid. Reprocess this data at a later time.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
A company wants to use AWS CloudFormation for infrastructure deployment. The company has strict tagging and resource requirements and wants to limit the deployment to two Regions. Developers will need to deploy multiple versions of the same application.Which solution ensures resources are deployed in accordance with company policy?

A. Create AWS Trusted Advisor checks to find and remediate unapproved CloudFormation StackSets.
B. Create a Cloud Formation drift detection operation to find and remediate unapproved CloudFormation StackSets.
C. Create CloudFormation StackSets with approved CloudFormation templates.
D. Create AWS Service Catalog products with approved CloudFormation templates.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
A company requires its developers to tag all Amazon Elastic Block Store (Amazon EBS) volumes in an account

to indicate a desired backup frequency. This requirement Includes EBS volumes that do not require backups. The company uses custom tags named Backup_Frequency that have values of none, dally, or weekly that correspond to the desired backup frequency. An audit finds that developers are occasionally not tagging the EBS volumes.A DevOps engineer needs to ensure that all EBS volumes always have the Backup_Frequency tag so that the company can perform backups at least weekly unless a different value is specified.Which solution will meet these requirements?

A. Set up AWS Config in the account. Create a custom rule that returns a compliance failure for all Amazon EC2 resources that do not have a Backup Frequency tag applied. Configure a remediation action that uses a custom AWS Systems Manager Automation runbook to apply the Backup_Frequency tag with a value of weekly.
B. Set up AWS Config in the account. Use a managed rule that returns a compliance failure for EC2::Volume resources that do not have a Backup Frequency tag applied. Configure a remediation action that uses a custom AWS Systems Manager Automation runbook to apply the Backup_Frequency tag with a value of weekly.
C. Turn on AWS CloudTrail in the account. Create an Amazon EventBridge rule that reacts to EBS CreateVolume events. Configure a custom AWS Systems Manager Automation runbook to apply the Backup_Frequency tag with a value of weekly. Specify the runbook as the target of the rule.
D. Turn on AWS CloudTrail in the account. Create an Amazon EventBridge rule that reacts to EBS CreateVolume events or EBS ModifyVolume events. Configure a custom AWS Systems Manager Automation runbook to apply the Backup_Frequency tag with a value of weekly. Specify the runbook as the target of the rule.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
A company requires that its internally facing web application be highly available. The architecture is made up of one Amazon EC2 web server instance and one NAT instance that provides outbound internet access for updates and accessing public data.Which combination of architecture adjustments should the company implement to achieve high availability? (Choose two.)

A. Add the NAT instance to an EC2 Auto Scaling group that spans multiple Availability Zones. Update the route tables.
B. Create additional EC2 instances spanning multiple Availability Zones. Add an Application Load Balancer to split the load between them.
C. Configure an Application Load Balancer in front of the EC2 instance. Configure Amazon CloudWatch alarms to recover the EC2 instance upon host failure.
D. Replace the NAT instance with a NAT gateway in each Availability Zone. Update the route tables.
E. Replace the NAT instance with a NAT gateway that spans multiple Availability Zones. Update the route tables.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
A DevOps engineer is building a multistage pipeline with AWS CodePipeline to build, verify, stage, test, and deploy an application. A manual approval stage is required between the test stage and the deploy stage. The development team uses a custom chat tool with webhook support that requires near-real-time

notifications.How should the DevOps engineer configure status updates for pipeline activity and approval requests to post to the chat tool?

A. Create an Amazon CloudWatch Logs subscription that filters on CodePipeline Pipeline Execution State Change. Publish subscription events to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the chat webhook URL to the SNS topic, and complete the subscription validation.
B. Create an AWS Lambda function that is invoked by AWS CloudTrail events. When a CodePipeline Pipeline Execution State Change event is detected, send the event details to the chat webhook UR
C. Create an Amazon EventBridge rule that filters on CodePipeline Pipeline Execution State Change. Publish the events to an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function that sends event details to the chat webhook UR
D. Modify the pipeline code to send the event details to the chat webhook URL at the end of each stage. Parameterize the URL so that each pipeline can send to a different URL based on the pipeline environment.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
A company's application development team uses Linux-based Amazon EC2 instances as bastion hosts. Inbound SSH access to the bastion hosts is restricted to specific IP addresses, as defined in the associated security groups. The company's security team wants to receive a notification if the security group rules are modified to allow SSH access from any IP address.What should a DevOps engineer do to meet this requirement?

A. Create an Amazon EventBridge rule with a source of aws.cloudtrail and the event name AuthorizeSecurityGroupIngress. Define an Amazon Simple Notification Service (Amazon SNS) topic as the target.
B. Enable Amazon GuardDuty and check the findings for security groups in AWS Security Hub. Configure an Amazon EventBridge rule with a custom pattern that matches GuardDuty events with an output of NON_COMPLIAN
C. Create an AWS Config rule by using the restricted-ssh managed rule to check whether security groups disallow unrestricted incoming SSH traffic. Configure automatic remediation to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
D. Enable Amazon Inspector. Include the Common Vulnerabilities and Exposures-1.1 rules package to check the security groups that are associated with the bastion hosts. Configure Amazon Inspector to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292
A DevOps team manages an API running on-premises that serves as a backend for an Amazon API Gateway endpoint. Customers have been complaining about high response latencies, which the development team has verified using the API Gateway latency metrics in Amazon CloudWatch. To identify the cause, the team needs to collect relevant data without introducing additional latency.Which actions should be taken to accomplish this? (Choose two.)

A. Install the CloudWatch agent server side and configure the agent to upload relevant logs to CloudWatch.

B. Enable AWS X-Ray tracing in API Gateway, modify the application to capture request segments, and upload those segments to X-Ray during each request.
C. Enable AWS X-Ray tracing in API Gateway, modify the application to capture request segments, and use the X-Ray daemon to upload segments to X-Ray.
D. Modify the on-premises application to send log information back to API Gateway with each request.
E. Modify the on-premises application to calculate and upload statistical data relevant to the API service requests to CloudWatch metrics.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293
A company has an application that is using a MySQL-compatible Amazon Aurora Multi-AZ DB cluster as the database. A cross-Region read replica has been created for disaster recovery purposes. A DevOps engineer wants to automate the promotion of the replica so it becomes the primary database instance in the event of a failure.Which solution will accomplish this?

A. Configure a latency-based Amazon Route 53 CNAME with health checks so it points to both the primary and replica endpoints. Subscribe an Amazon SNS topic to Amazon RDS failure notifications from AWS CloudTrail and use that topic to invoke an AWS Lambda function that will promote the replica instance as the primary.
B. Create an Aurora custom endpoint to point to the primary database instance. Configure the application to use this endpoint. Configure AWS CloudTrail to run an AWS Lambda function to promote the replica instance and modify the custom endpoint to point to the newly promoted instance.
C. Create an AWS Lambda function to modify the application's AWS CloudFormation template to promote the replica, apply the template to update the stack, and point the application to the newly promoted instance. Create an Amazon CloudWatch alarm to invoke this Lambda function after the failure event occurs.
D. Store the Aurora endpoint in AWS Systems Manager Parameter Store. Create an Amazon EventBridge event that detects the database failure and runs an AWS Lambda function to promote the replica instance and update the endpoint URL stored in AWS Systems Manager Parameter Store. Code the application to reload the endpoint from Parameter Store if a database connection fails.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
A company hosts its staging website using an Amazon EC2 instance backed with Amazon EBS storage. The company wants to recover quickly with minimal data losses in the event of network connectivity issues or power failures on the EC2 instance.Which solution will meet these requirements?

A. Add the instance to an EC2 Auto Scaling group with the minimum, maximum, and desired capacity set to 1.
B. Add the instance to an EC2 Auto Scaling group with a lifecycle hook to detach the EBS volume when the EC2 instance shuts down or terminates.
C. Create an Amazon CloudWatch alarm for the StatusCheckFailed System metric and select the EC2 action to recover the instance.
D. Create an Amazon CloudWatch alarm for the StatusCheckFailed Instance metric and select the EC2 action to reboot the instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
A company wants to use AWS development tools to replace its current bash deployment scripts. The company currently deploys a LAMP application to a group of Amazon EC2 instances behind an Application Load Balancer (ALB). During the deployments, the company unit tests the committed application, stops and starts services, unregisters and re-registers instances with the load balancer, and updates file permissions. The company wants to maintain the same deployment functionality through the shift to using AWS services.Which solution will meet these requirements?

A. Use AWS CodeBuild to test the application. Use bash scripts invoked by AWS CodeDeploy's appspec.yml file to restart services, and deregister and register instances with the AL
B. Use the appspec.yml file to update file permissions without a custom script.
C. Use AWS CodePipeline to move the application source code from the AWS CodeCommit repository to AWS CodeDeploy. Use CodeDeploy to test the application. Use CodeDeploy's appspec.yml file to restart services and update permissions without a custom script. Use AWS CodeBuild to unregister and re-register instances with the AL
D. Use AWS CodePipeline to trigger AWS CodeBuild to test the application. Use bash scripts invoked by AWS CodeDeploy's appspec.yml file to restart services. Unregister and re-register the instances in the AWS CodeDeploy deployment group with the AL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296
A company runs an application with an Amazon EC2 and on-premises configuration. A DevOps engineer needs to standardize patching across both environments. Company policy dictates that patching only happens during non-business hours.Which combination of actions will meet these requirements? (Choose three.)

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

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297
A company has chosen AWS to host a new application. The company needs to implement a multi-account strategy. A DevOps engineer creates a new AWS account and an organization in AWS Organizations. The DevOps engineer also creates the OU structure for the organization and sets up a landing zone by using AWS Control Tower.The DevOps engineer must implement a solution that automatically deploys resources for new

accounts that users create through AWS Control Tower Account Factory. When a user creates a new account, the solution must apply AWS CloudFormation templates and SCPs that are customized for the OU or the account to automatically deploy all the resources that are attached to the account. All the OUs are enrolled in AWS Control Tower.Which solution will meet these requirements in the MOST automated way?

A. Use AWS Service Catalog with AWS Control Tower. Create portfolios and products in AWS Service Catalog. Grant granular permissions to provision these resources. Deploy SCPs by using the AWS CLI and JSON documents.
B. Deploy CloudFormation stack sets by using the required templates. Enable automatic deployment. Deploy stack instances to the required accounts. Deploy a CloudFormation stack set to the organizationâ€™s management account to deploy SCPs.
C. Create an Amazon EventBridge rule to detect the CreateManagedAccount event. Configure AWS Service Catalog as the target to deploy resources to any new accounts. Deploy SCPs by using the AWS CLI and JSON documents.
D. Deploy the Customizations for AWS Control Tower (CfCT) solution. Use an AWS CodeCommit repository as the source. In the repository, create a custom package that includes the CloudFormation templates and the SCP JSON documents.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
An online retail company based in the United States plans to expand its operations to Europe and Asia in the next six months. Its product currently runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. All data is stored in an Amazon Aurora database instance.When the product is deployed in multiple regions, the company wants a single product catalog across all regions, but for compliance purposes, its customer information and purchases must be kept in each region.How should the company meet these requirements with the LEAST amount of application changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
A company is using an Amazon Aurora cluster as the data store for its application. The Aurora cluster is configured with a single DB instance. The application performs read and write operations on the database by using the cluster's instance endpoint.The company has scheduled an update to be applied to the cluster during an upcoming maintenance window. The cluster must remain available with the least possible interruption during the maintenance window.What should a DevOps engineer do to meet these requirements?

A. Add a reader instance to the Aurora cluster. Update the application to use the Aurora cluster endpoint for write operations. Update the Aurora cluster's reader endpoint for reads.
B. Add a reader instance to the Aurora cluster. Create a custom ANY endpoint for the cluster. Update the application to use the Aurora cluster's custom ANY endpoint for read and write operations.
C. Turn on the Multi-AZ option on the Aurora cluster. Update the application to use the Aurora cluster endpoint for write operations. Update the Aurora clusterâ€™s reader endpoint for reads.
D. Turn on the Multi-AZ option on the Aurora cluster. Create a custom ANY endpoint for the cluster. Update the application to use the Aurora cluster's custom ANY endpoint for read and write operations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
A company is implementing a well-architected design for its globally accessible API stack. The design needs to ensure both high reliability and fast response times for users located in North America and Europe.The API stack contains the following three tiers:Amazon API Gateway -AWS Lambda -Amazon DynamoDB -Which solution will meet the requirements?

A. Configure Amazon Route 53 to point to API Gateway APIs in North America and Europe using health checks. Configure the APIs to forward requests to a Lambda function in that Region. Configure the Lambda functions to retrieve and update the data in a DynamoDB table in the same Region as the Lambda function.
B. Configure Amazon Route 53 to point to API Gateway APIs in North America and Europe using latency-based routing and health checks. Configure the APIs to forward requests to a Lambda function in that Region. Configure the Lambda functions to retrieve and update the data in a DynamoDB global table.
C. Configure Amazon Route 53 to point to API Gateway in North America, create a disaster recovery API in Europe, and configure both APIs to forward requests to the Lambda functions in that Region. Retrieve the data from a DynamoDB global table. Deploy a Lambda function to check the North America API health every 5 minutes. In the event of a failure, update Route 53 to point to the disaster recovery AP
D. Configure Amazon Route 53 to point to API Gateway API in North America using latency-based routing. Configure the API to forward requests to the Lambda function in the Region nearest to the user. Configure the Lambda function to retrieve and update the data in a DynamoDB table.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301
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 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 teamâ€™s template. To retrieve Virtual Private Cloud (VPC) and subnet values, use Fn::ImportValue intrinsic functions in the Parameters section of the root 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 root 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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 302
A company uses AWS Organizations to manage multiple accounts. Information security policies require that all unencrypted Amazon EBS volumes be marked as non-compliant. A DevOps engineer needs to automatically deploy the solution and ensure that this compliance check is always present.Which solution will accomplish this?

A. Create an AWS CloudFormation template that defines an AWS Inspector rule to check whether EBS encryption is enabled. Save the template to an Amazon S3 bucket that has been shared with all accounts within the company. Update the account creation script pointing to the CloudFormation template in Amazon S3.

B. Create an AWS Config organizational rule to check whether EBS encryption is enabled and deploy the rule using the AWS CL

C. Create an SCP in Organizations. Set the policy to prevent the launch of Amazon EC2 instances without encryption on the EBS volumes using a conditional expression. Apply the SCP to all AWS accounts. Use Amazon Athena to analyze the AWS CloudTrail output, looking for events that deny an ec2:RunInstances action.

D. Deploy an IAM role to all accounts from a single trusted account. Build a pipeline with AWS CodePipeline with a stage in AWS Lambda to assume the IAM role, and list all EBS volumes in the account. Publish a report to Amazon S3.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 303
A company is performing vulnerability scanning for all Amazon EC2 instances across many accounts. The accounts are in an organization in AWS Organizations. Each account's VPCs are attached to a shared transit gateway. The VPCs send traffic to the internet through a central egress VPC. The company has enabled Amazon Inspector in a delegated administrator account and has enabled scanning for all member accounts.A DevOps engineer discovers that some EC2 instances are listed in the "not scanning" tab in Amazon Inspector.Which combination of actions should the DevOps engineer take to resolve this issue? (Choose three.)

A. Verify that AWS Systems Manager Agent is installed and is running on the EC2 instances that Amazon Inspector is not scanning.
B. Associate the target EC2 instances with security groups that allow outbound communication on port 443 to the AWS Systems Manager service endpoint.
C. Grant inspector:StartAssessmentRun permissions to the IAM role that the DevOps engineer is using.
D. Configure EC2 Instance Connect for the EC2 instances that Amazon Inspector is not scanning.
E. Associate the target EC2 instances with instance profiles that grant permissions to communicate with AWS Systems Manager.
F. Create a managed-instance activation. Use the Activation Code and the Activation ID to register the EC2 instances.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304
A development team uses AWS CodeCommit for version control for applications. The development team uses AWS CodePipeline, AWS CodeBuild. and AWS CodeDeploy for CI/CD infrastructure. In CodeCommit, the development team recently merged pull requests that did not pass long-running tests in the code base. The development team needed to perform rollbacks to branches in the codebase, resulting in lost time and wasted effort.A DevOps engineer must automate testing of pull requests in CodeCommit to ensure that reviewers more easily see the results of automated tests as part of the pull request review.What should the DevOps engineer do to meet this requirement?

A. Create an Amazon EventBridge rule that reacts to the pullRequestStatusChanged event. Create an AWS Lambda function that invokes a CodePipeline pipeline with a CodeBuild action that runs the tests for the application. Program the Lambda function to post the CodeBuild badge as a comment on the pull request so that developers will see the badge in their code review.
B. Create an Amazon EventBridge rule that reacts to the pullRequestCreated event. Create an AWS Lambda function that invokes a CodePipeline pipeline with a CodeBuild action that runs the tests for the application. Program the Lambda function to post the CodeBuild test results as a comment on the pull request when the test results are complete.
C. Create an Amazon EventBridge rule that reacts to pullRequestCreated and pullRequestSourceBranchUpdated events. Create an AWS Lambda function that invokes a CodePipeline pipeline with a CodeBuild action that runs the tests for the application. Program the Lambda function to post the CodeBuild badge as a comment on the pull request so that developers will see the badge in their code review.
D. Create an Amazon EventBridge rule that reacts to the pullRequestStatusChanged event. Create an AWS Lambda function that invokes a CodePipeline pipeline with a CodeBuild action that runs the tests for the application. Program the Lambda function to post the CodeBuild test results as a comment on the pull request when the test results are complete.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
A company has deployed an application in a production VPC in a single AWS account. The application is popular and is experiencing heavy usage. The companyâ€™s security team wants to add additional security, such as AWS WAF, to the application deployment. However, the application's product manager is concerned about cost and does not want to approve the change unless the security team can prove that additional security

is necessary.The security team believes that some of the application's demand might come from users that have IP addresses that are on a deny list. The security team provides the deny list to a DevOps engineer. If any of the IP addresses on the deny list access the application, the security team wants to receive automated notification in near real time so that the security team can document that the application needs additional security. The DevOps engineer creates a VPC flow log for the production VPC.Which set of additional steps should the DevOps engineer take to meet these requirements MOST cost-effectively?

A. Create a log group in Amazon CloudWatch Logs. Configure the VPC flow log to capture accepted traffic and to send the data to the log group. Create an Amazon CloudWatch metric filter for IP addresses on the deny list. Create a CloudWatch alarm with the metric filter as input. Set the period to 5 minutes and the datapoints to alarm to 1. Use an Amazon Simple Notification Service (Amazon SNS) topic to send alarm notices to the security team.
B. Create an Amazon S3 bucket for log files. Configure the VPC flow log to capture all traffic and to send the data to the S3 bucket. Configure Amazon Athena to return all log files in the S3 bucket for IP addresses on the deny list. Configure Amazon QuickSight to accept data from Athena and to publish the data as a dashboard that the security team can access. Create a threshold alert of 1 for successful access. Configure the alert to automatically notify the security team as frequently as possible when the alert threshold is met.
C. Create an Amazon S3 bucket for log files. Configure the VPC flow log to capture accepted traffic and to send the data to the S3 bucket. Configure an Amazon OpenSearch Service cluster and domain for the log files. Create an AWS Lambda function to retrieve the logs from the S3 bucket, format the logs, and load the logs into the OpenSearch Service cluster. Schedule the Lambda function to run every 5 minutes. Configure an alert and condition in OpenSearch Service to send alerts to the security team through an Amazon Simple Notification Service (Amazon SNS) topic when access from the IP addresses on the deny list is detected.
D. Create a log group in Amazon CloudWatch Logs. Create an Amazon S3 bucket to hold query results. Configure the VPC flow log to capture all traffic and to send the data to the log group. Deploy an Amazon Athena CloudWatch connector in AWS Lambda. Connect the connector to the log group. Configure Athena to periodically query for all accepted traffic from the IP addresses on the deny list and to store the results in the S3 bucket. Configure an S3 event notification to automatically notify the security team through an Amazon Simple Notification Service (Amazon SNS) topic when new objects are added to the S3 bucket.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306
A DevOps engineer has automated a web service deployment by using AWS CodePipeline with the following steps:1. An AWS CodeBuild project compiles the deployment artifact and runs unit tests.2. An AWS CodeDeploy deployment group deploys the web service to Amazon EC2 instances in the staging environment.3. A CodeDeploy deployment group deploys the web service to EC2 instances in the production environment.The quality assurance (QA) team requests permission to inspect the build artifact before the deployment to the production environment occurs. The QA team wants to run an internal penetration testing tool to conduct manual tests. The tool will be invoked by a REST API call.Which combination of actions should the DevOps engineer take to fulfill this request? (Choose two.)

A. Insert a manual approval action between the test actions and deployment actions of the pipeline.
B. Modify the buildspec.yml file for the compilation stage to require manual approval before completion.
C. Update the CodeDeploy deployment groups so that they require manual approval to proceed.
D. Update the pipeline to directly call the REST API for the penetration testing tool.
E. Update the pipeline to invoke an AWS Lambda function that calls the REST API for the penetration testing tool.

Correct Answer: AE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 307
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 for 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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 308
A company runs an application on Amazon EC2 instances. The company uses a series of AWS CloudFormation stacks to define the application resources. A developer performs updates by building and testing the application on a laptop and then uploading the build output and CloudFormation stack templates to Amazon S3. The developer's peers review the changes before the developer performs the CloudFormation stack update and installs a new version of the application onto the EC2 instances.The deployment process is prone to errors and is time-consuming when the developer updates each EC2 instance with the new application. The company wants to automate as much of the application deployment process as possible while retaining a final manual approval step before the modification of the application or resources.The company already has moved the source code for the application and the CloudFormation templates to AWS CodeCommit. The company also has created an AWS CodeBuild project to build and test the application.Which combination of steps will meet the companyâ€™s requirements? (Choose two.)

A. Create an application group and a deployment group in AWS CodeDeploy. Install the CodeDeploy agent on the EC2 instances.
B. Create an application revision and a deployment group in AWS CodeDeploy. Create an environment in CodeDeploy. Register the EC2 instances to the CodeDeploy environment.
C. Use AWS CodePipeline to invoke the CodeBuild job, run the CloudFormation update, and pause for a manual approval step. After approval, start the AWS CodeDeploy deployment.
D. Use AWS CodePipeline to invoke the CodeBuild job, create CloudFormation change sets for each of the application stacks, and pause for a manual approval step. After approval, run the CloudFormation change sets and start the AWS CodeDeploy deployment.
E. Use AWS CodePipeline to invoke the CodeBuild job, create CloudFormation change sets for each of the application stacks, and pause for a manual approval step. After approval, start the AWS CodeDeploy deployment.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 309
A DevOps engineer manages a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group across multiple Availability Zones. The engineer needs to implement a deployment strategy that:Launches a second fleet of instances with the same capacity as the original fleet.Maintains the original fleet unchanged while the second fleet is launched.Transitions traffic to the second fleet when the second fleet is fully deployed.Terminates the original fleet automatically 1 hour after transition.Which solution will satisfy these requirements?

A. Use an AWS CloudFormation template with a retention policy for the ALB set to 1 hour. Update the Amazon Route 53 record to reflect the new AL
B.
C. Use AWS CodeDeploy with a deployment group configured with a blue/green deployment configuration Select the option Terminate the original instances in the deployment group with a waiting period of 1 hour.
D. Use AWS Elastic Beanstalk with the configuration set to Immutable. Create an .ebextension using the Resources key that sets the deletion policy of the ALB to 1 hour, and deploy the application.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310
A company must encrypt all AMIs that the company shares across accounts. A DevOps engineer has access to a source account where an unencrypted custom AMI has been built. The DevOps engineer also has access to a target account where an Amazon EC2 Auto Scaling group will launch EC2 instances from the AMI. The DevOps engineer must share the AMI with the target account.The company has created an AWS Key Management Service (AWS KMS) key in the source account.Which additional steps should the DevOps engineer perform to meet the requirements? (Choose three.)

A. In the source account, copy the unencrypted AMI to an encrypted AM
B. In the source account, copy the unencrypted AMI to an encrypted AM
C. In the source account, create a KMS grant that delegates permissions to the Auto Scaling group service-linked role in the target account.
D. In the source account, modify the key policy to give the target account permissions to create a grant. In the target account, create a KMS grant that delegates permissions to the Auto Scaling group service-linked role.
E. In the source account, share the unencrypted AMI with the target account.
F. In the source account, share the encrypted AMI with the target account.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311

A video-sharing company stores its videos in Amazon S3. The company has observed a sudden increase in video access requests, but the company does not know which videos are most popular. The company needs to identify the general access pattern for the video files. This pattern includes the number of users who access a certain file on a given day, as well as the number of pull requests for certain files.How can the company meet these requirements with the LEAST amount of effort?

A. Activate S3 server access logging. Import the access logs into an Amazon Aurora database. Use an Aurora SQL query to analyze the access patterns.
B. Activate S3 server access logging. Use Amazon Athena to create an external table with the log files. Use Athena to create a SQL query to analyze the access patterns.
C. Invoke an AWS Lambda function for every S3 object access event. Configure the Lambda function to write the file access information, such as user. S3 bucket, and file key, to an Amazon Aurora database. Use an Aurora SQL query to analyze the access patterns.
D. Record an Amazon CloudWatch Logs log message for every S3 object access event. Configure a CloudWatch Logs log stream to write the file access information, such as user, S3 bucket, and file key, to an Amazon Kinesis Data Analytics for SQL application. Perform a sliding window analysis.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312
A development team wants to use AWS CloudFormation stacks to deploy an application. However, the developer IAM role does not have the required permissions to provision the resources that are specified in the AWS CloudFormation template. A DevOps engineer needs to implement a solution that allows the developers to deploy the stacks. The solution must follow the principle of least privilege.Which solution will meet these requirements?

A. Create an IAM policy that allows the developers to provision the required resources. Attach the policy to the developer IAM role.
B. Create an IAM policy that allows full access to AWS CloudFormation. Attach the policy to the developer IAM role.
C. Create an AWS CloudFormation service role that has the required permissions. Grant the developer IAM role a cloudformation:* action. Use the new service role during stack deployments.
D. Create an AWS CloudFormation service role that has the required permissions. Grant the developer IAM role the iam:PassRole permission. Use the new service role during stack deployments.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 313
A production account has a requirement that any Amazon EC2 instance that has been logged in to manually must be terminated within 24 hours. All applications in the production account are using Auto Scaling groups with the Amazon CloudWatch Logs agent configured.How can this process be automated?

A. Create a CloudWatch Logs subscription to an AWS Step Functions application. Configure an AWS Lambda function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned. Create an Amazon EventBridge rule to invoke a second Lambda function once a day that will terminate all instances with this tag.
B. Create an Amazon CloudWatch alarm that will be invoked by the login event. Send the notification to an

Amazon Simple Notification Service (Amazon SNS) topic that the operations team is subscribed to, and have them terminate the EC2 instance within 24 hours.

C. Create an Amazon CloudWatch alarm that will be invoked by the login event. Configure the alarm to send to an Amazon Simple Queue Service (Amazon SQS) queue. Use a group of worker instances to process messages from the queue, which then schedules an Amazon EventBridge rule to be invoked.

D. Create a CloudWatch Logs subscription to 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 an Amazon EventBridge rule to invoke a daily Lambda function that terminates all instances with this tag.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314
A company has enabled all features for its organization in AWS Organizations. The organization contains 10 AWS accounts. The company has turned on AWS CloudTrail in all the accounts. The company expects the number of AWS accounts in the organization to increase to 500 during the next year. The company plans to use multiple OUs for these accounts.The company has enabled AWS Config in each existing AWS account in the organization. A DevOps engineer must implement a solution that enables AWS Config automatically for all future AWS accounts that are created in the organization.Which solution will meet this requirement?

A. In the organization's management account, create an Amazon EventBridge rule that reacts to a CreateAccount API call. Configure the rule to invoke an AWS Lambda function that enables trusted access to AWS Config for the organization.

B. In the organization's management account, create an AWS CloudFormation stack set to enable AWS Config. Configure the stack set to deploy automatically when an account is created through Organizations.

C. In the organization's management account, create an SCP that allows the appropriate AWS Config API calls to enable AWS Config. Apply the SCP to the root-level O

D. In the organization's management account, create an Amazon EventBridge rule that reacts to a CreateAccount API call. Configure the rule to invoke an AWS Systems Manager Automation runbook to enable AWS Config for the account.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315
A company has many applications. Different teams in the company developed the applications by using multiple languages and frameworks. The applications run on premises and on different servers with different operating systems. Each team has its own release protocol and process. The company wants to reduce the complexity of the release and maintenance of these applications.The company is migrating its technology stacks, including these applications, to AWS. The company wants centralized control of source code, a consistent and automatic delivery pipeline, and as few maintenance tasks as possible on the underlying infrastructure.What should a DevOps engineer do to meet these requirements?

A. Create one AWS CodeCommit repository for all applications. Put each application's code in a different branch. Merge the branches, and use AWS CodeBuild to build the applications. Use AWS CodeDeploy to deploy the applications to one centralized application server.

B. Create one AWS CodeCommit repository for each of the applications. Use AWS CodeBuild to build the applications one at a time. Use AWS CodeDeploy to deploy the applications to one centralized application server.

C. Create one AWS CodeCommit repository for each of the applications. Use AWS CodeBuild to build the applications one at a time and to create one AMI for each server. Use AWS CloudFormation StackSets to automatically provision and decommission Amazon EC2 fleets by using these AMIs.
D. Create one AWS CodeCommit repository for each of the applications. Use AWS CodeBuild to build one Docker image for each application in Amazon Elastic Container Registry (Amazon ECR). Use AWS CodeDeploy to deploy the applications to Amazon Elastic Container Service (Amazon ECS) on infrastructure that AWS Fargate manages.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
A company uses AWS CodePipeline pipelines to automate releases of its application A typical pipeline consists of three stages build, test, and deployment. The company has been using a separate AWS CodeBuild project to run scripts for each stage. However, the company now wants to use AWS CodeDeploy to handle the deployment stage of the pipelines.The company has packaged the application as an RPM package and must deploy the application to a fleet of Amazon EC2 instances. The EC2 instances are in an EC2 Auto Scaling group and are launched from a common AMI.Which combination of steps should a DevOps engineer perform to meet these requirements? (Choose two.)

A. Create a new version of the common AMI with the CodeDeploy agent installed. Update the IAM role of the EC2 instances to allow access to CodeDeploy.
B. Create a new version of the common AMI with the CodeDeploy agent installed. Create an AppSpec file that contains application deployment scripts and grants access to CodeDeploy.
C. Create an application in CodeDeploy. Configure an in-place deployment type. Specify the Auto Scaling group as the deployment target. Add a step to the CodePipeline pipeline to use EC2 Image Builder to create a new AM
D. Create an application in CodeDeploy. Configure an in-place deployment type. Specify the Auto Scaling group as the deployment target. Update the CodePipeline pipeline to use the CodeDeploy action to deploy the application.
E. Create an application in CodeDeploy. Configure an in-place deployment type. Specify the EC2 instances that are launched from the common AMI as the deployment target. Update the CodePipeline pipeline to use the CodeDeploy action to deploy the application.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
A company has an application that runs on a fleet of Amazon EC2 instances. The application requires frequent restarts. The application logs contain error messages when a restart is required. The application logs are published to a log group in Amazon CloudWatch Logs.An Amazon CloudWatch alarm notifies an application engineer through an Amazon Simple Notification Service (Amazon SNS) topic when the logs contain a large number of restart-related error messages. The application engineer manually restarts the application on the instances after the application engineer receives a notification from the SNS topic.A DevOps engineer needs to implement a solution to automate the application restart on the instances without restarting the instances.Which solution will meet these requirements in the MOST operationally efficient manner?

A. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instances. Configure the SNS topic to invoke the runbook.

B. Create an AWS Lambda function that restarts the application on the instances. Configure the Lambda function as an event destination of the SNS topic.
C. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instances. Create an AWS Lambda function to invoke the runbook. Configure the Lambda function as an event destination of the SNS topic.
D. Configure an AWS Systems Manager Automation runbook that runs a script to restart the application on the instances. Configure an Amazon EventBridge rule that reacts when the CloudWatch alarm enters ALARM state. Specify the runbook as a target of the rule.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318
A DevOps engineer at a company is supporting an AWS environment in which all users use AWS IAM Identity Center (AWS Single Sign-On). The company wants to immediately disable credentials of any new IAM user and wants the security team to receive a notification.Which combination of steps should the DevOps engineer take to meet these requirements? (Choose three.)

A. Create an Amazon EventBridge rule that reacts to an IAM CreateUser API call in AWS CloudTrail.
B. Create an Amazon EventBridge rule that reacts to an IAM GetLoginProfile API call in AWS CloudTrail.
C. Create an AWS Lambda function that is a target of the EventBridge rule. Configure the Lambda function to disable any access keys and delete the login profiles that are associated with the IAM user.
D. Create an AWS Lambda function that is a target of the EventBridge rule. Configure the Lambda function to delete the login profiles that are associated with the IAM user.
E. Create an Amazon Simple Notification Service (Amazon SNS) topic that is a target of the EventBridge rule. Subscribe the security team's group email address to the topic.
F. Create an Amazon Simple Queue Service (Amazon SQS) queue that is a target of the Lambda function. Subscribe the security team's group email address to the queue.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 319
A company wants to set up a continuous delivery pipeline. The company stores application code in a private GitHub repository. The company needs to deploy the application components to Amazon Elastic Container Service (Amazon ECS). Amazon EC2, and AWS Lambda. The pipeline must support manual approval actions.Which solution will meet these requirements?

A. Use AWS CodePipeline with Amazon EC
B. Use AWS CodePipeline with AWS CodeDeploy as the deploy provider.
C. Use AWS CodePipeline with AWS Elastic Beanstalk as the deploy provider.
D. Use AWS CodeDeploy with GitHub integration to deploy the application.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320
A company has an application that runs on Amazon EC2 instances that are in an Auto Scaling group. When the application starts up. the application needs to process data from an Amazon S3 bucket before the application can start to serve requests.The size of the data that is stored in the S3 bucket is growing. When the Auto Scaling group adds new instances, the application now takes several minutes to download and process the data before the application can serve requests. The company must reduce the time that elapses before new EC2 instances are ready to serve requests.Which solution is the MOST cost-effective way to reduce the application startup time?

A. Configure a warm pool for the Auto Scaling group with warmed EC2 instances in the Stopped state. Configure an autoscaling:EC2_INSTANCE_LAUNCHING lifecycle hook on the Auto Scaling group. Modify the application to complete the lifecycle hook when the application is ready to serve requests.
B. Increase the maximum instance count of the Auto Scaling group. Configure an autoscaling:EC2_INSTANCE_LAUNCHING lifecycle hook on the Auto Scaling group. Modify the application to complete the lifecycle hook when the application is ready to serve requests.
C. Configure a warm pool for the Auto Scaling group with warmed EC2 instances in the Running state. Configure an autoscaling:EC2_INSTANCE_LAUNCHING lifecycle hook on the Auto Scaling group. Modify the application to complete the lifecycle hook when the application is ready to serve requests.
D. Increase the maximum instance count of the Auto Scaling group. Configure an autoscaling:EC2_INSTANCE_LAUNCHING lifecycle hook on the Auto Scaling group. Modify the application to complete the lifecycle hook and to place the new instance in the Standby state when the application is ready to serve requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321
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: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 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 â€œ*â€.
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
A company has developed a serverless web application that is hosted on AWS. The application consists of Amazon S3. Amazon API Gateway, several AWS Lambda functions, and an Amazon RDS for MySQL

database. The company is using AWS CodeCommit to store the source code. The source code is a combination of AWS Serverless Application Model (AWS SAM) templates and Python code.A security audit and penetration test reveal that user names and passwords for authentication to the database are hardcoded within CodeCommit repositories. A DevOps engineer must implement a solution to automatically detect and prevent hardcoded secrets.What is the MOST secure solution that meets these requirements?

A. Enable Amazon CodeGuru Profiler. Decorate the handler function with @with_lambda_profiler(). Manually review the recommendation report. Write the secret to AWS Systems Manager Parameter Store as a secure string. Update the SAM templates and the Python code to pull the secret from Parameter Store.
B. Associate the CodeCommit repository with Amazon CodeGuru Reviewer. Manually check the code review for any recommendations. Choose the option to protect the secret. Update the SAM templates and the Python code to pull the secret from AWS Secrets Manager.
C. Enable Amazon CodeGuru Profiler. Decorate the handler function with @with_lambda_profiler(). Manually review the recommendation report. Choose the option to protect the secret. Update the SAM templates and the Python code to pull the secret from AWS Secrets Manager.
D. Associate the CodeCommit repository with Amazon CodeGuru Reviewer. Manually check the code review for any recommendations. Write the secret to AWS Systems Manager Parameter Store as a string. Update the SAM templates and the Python code to pull the secret from Parameter Store.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 323
A company is using Amazon S3 buckets to store important documents. The company discovers that some S3 buckets are not encrypted. Currently, the companyâ€™s IAM users can create new S3 buckets without encryption. The company is implementing a new requirement that all S3 buckets must be encrypted.A DevOps engineer must implement a solution to ensure that server-side encryption is enabled on all existing S3 buckets and all new S3 buckets. The encryption must be enabled on new S3 buckets as soon as the S3 buckets are created. The default encryption type must be 256-bit Advanced Encryption Standard (AES-256).Which solution will meet these requirements?

A. Create an AWS Lambda function that is invoked periodically by an Amazon EventBridge scheduled rule. Program the Lambda function to scan all current S3 buckets for encryption status and to set AES-256 as the default encryption for any S3 bucket that does not have an encryption configuration.
B. Set up and activate the s3-bucket-server-side-encryption-enabled AWS Config managed rule. Configure the rule to use the AWS-EnableS3BucketEncryption AWS Systems Manager Automation runbook as the remediation action. Manually run the re-evaluation process to ensure that existing S3 buckets are compliant.
C. Create an AWS Lambda function that is invoked by an Amazon EventBridge event rule. Define the rule with an event pattern that matches the creation of new S3 buckets. Program the Lambda function to parse the EventBridge event, check the configuration of the S3 buckets from the event, and set AES-256 as the default encryption.
D. Configure an IAM policy that denies the s3:CreateBucket action if the s3:x-amz-server-side-encryption condition key has a value that is not AES-256. Create an IAM group for all the companyâ€™s IAM users. Associate the IAM policy with the IAM group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 325
A company is hosting a static website from an Amazon S3 bucket. The website is available to customers at example.com. The company uses an Amazon Route 53 weighted routing policy with a TTL of 1 day. The company has decided to replace the existing static website with a dynamic web application. The dynamic web application uses an Application Load Balancer (ALB) in front of a fleet of Amazon EC2 instances.On the day of production launch to customers, the company creates an additional Route 53 weighted DNS record entry that points to the ALB with a weight of 255 and a TTL of 1 hour. Two days later, a DevOps engineer notices that the previous static website is displayed sometimes when customers navigate to example.com.How can the DevOps engineer ensure that the company serves only dynamic content for example.com?

A. Delete all objects, including previous versions, from the S3 bucket that contains the static website content.
B. Update the weighted DNS record entry that points to the S3 bucket. Apply a weight of 0. Specify the domain reset option to propagate changes immediately.
C. Configure webpage redirect requests on the S3 bucket with a hostname that redirects to the AL
D. Remove the weighted DNS record entry that points to the S3 bucket from the example.com hosted zone. Wait for DNS propagation to become complete.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 326
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 EventBridge:Which type of events will match this event pattern?

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

D. Approval actions across all the pipelines

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327
A companyâ€™s security team requires that all external Application Load Balancers (ALBs) and Amazon API Gateway APIs are associated with AWS WAF web ACLs. The company has hundreds of AWS accounts, all of which are included in a single organization in AWS Organizations. The company has configured AWS Config for the organization. During an audit, the company finds some externally facing ALBs that are not associated with AWS WAF web ACLs.Which combination of steps should a DevOps engineer take to prevent future violations? (Choose two.)

A. Delegate AWS Firewall Manager to a security account.
B. Delegate Amazon GuardDuty to a security account.
C. Create an AWS Firewall Manager policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
D. Create an Amazon GuardDuty policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.
E. Configure an AWS Config managed rule to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
An application running on a set of Amazon EC2 instances in an Auto Scaling group requires a configuration file to operate. The instances are created and maintained with AWS CloudFormation. A DevOps engineer wants the instances to have the latest configuration file when launched, and wants changes to the configuration file to be reflected on all the instances with a minimal delay when the CloudFormation template is updated. Company policy requires that application configuration files be maintained along with AWS infrastructure configuration files in source control.Which solution will accomplish this?

A. In the CloudFormation template, add an AWS Config rule. Place the configuration file content in the ruleâ €™s InputParameters property, and set the Scope property to the EC2 Auto Scaling group. Add an AWS Systems Manager Resource Data Sync resource to the template to poll for updates to the configuration.
B. In the CloudFormation template, add an EC2 launch template resource. Place the configuration file content in the launch template. Configure the cfn-init script to run when the instance is launched, and configure the cfn-hup script to poll for updates to the configuration.
C. In the CloudFormation template, add an EC2 launch template resource. Place the configuration file content in the launch template. Add an AWS Systems Manager Resource Data Sync resource to the template to poll for updates to the configuration.
D. In the CloudFormation template, add CloudFormation init metadata. Place the configuration file content in the metadata. Configure the cfn-init script to run when the instance is launched, and configure the cfn-hup script to poll for updates to the configuration.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 329
A company manages an application that stores logs in Amazon CloudWatch Logs. The company wants to archive the logs to an Amazon S3 bucket. Logs are rarely accessed after 90 days and must be retained for 10 years.Which combination of steps should a DevOps engineer take to meet these requirements? (Choose two.)

A. Configure a CloudWatch Logs subscription filter to use AWS Glue to transfer all logs to an S3 bucket.
B. Configure a CloudWatch Logs subscription filter to use Amazon Kinesis Data Firehose to stream all logs to an S3 bucket.
C. Configure a CloudWatch Logs subscription filter to stream all logs to an S3 bucket.
D. Configure the S3 bucket lifecycle policy to transition logs to S3 Glacier after 90 days and to expire logs after 3.650 days.
E. Configure the S3 bucket lifecycle policy to transition logs to Reduced Redundancy after 90 days and to expire logs after 3.650 days.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330
A company is developing a new application. The application uses AWS Lambda functions for its compute tier. The company must use a canary deployment for any changes to the Lambda functions. Automated rollback must occur if any failures are reported.The companyâ€™s DevOps team needs to create the infrastructure as code (IaC) and the CI/CD pipeline for this solution.Which combination of steps will meet these requirements? (Choose three.)

A. Create an AWS CloudFormation template for the application. Define each Lambda function in the template by using the AWS::Lambda::Function resource type. In the template, include a version for the Lambda function by using the AWS::Lambda::Version resource type. Declare the CodeSha256 property. Configure an AWS::Lambda::Alias resource that references the latest version of the Lambda function.
B. Create an AWS Serverless Application Model (AWS SAM) template for the application. Define each Lambda function in the template by using the AWS::Serverless::Function resource type. For each function, include configurations for the AutoPublishAlias property and the DeploymentPreference property. Configure the deployment configuration type to LambdaCanary10Percent10Minutes.
C. Create an AWS CodeCommit repository. Create an AWS CodePipeline pipeline. Use the CodeCommit repository in a new source stage that starts the pipeline. Create an AWS CodeBuild project to deploy the AWS Serverless Application Model (AWS SAM) template. Upload the template and source code to the CodeCommit repository. In the CodeCommit repository, create a buildspec.yml file that includes the commands to build and deploy the SAM application.
D. Create an AWS CodeCommit repository. Create an AWS CodePipeline pipeline. Use the CodeCommit repository in a new source stage that starts the pipeline. Create an AWS CodeDeploy deployment group that is configured for canary deployments with a DeploymentPreference type of Canary10Percent10Minutes. Upload the AWS CloudFormation template and source code to the CodeCommit repository. In the CodeCommit repository, create an appspec.yml file that includes the commands to deploy the CloudFormation template.
E. Create an Amazon CloudWatch composite alarm for all the Lambda functions. Configure an evaluation period and dimensions for Lambda. Configure the alarm to enter the ALARM state if any errors are detected or if there is insufficient data.
F. Create an Amazon CloudWatch alarm for each Lambda function. Configure the alarms to enter the ALARM state if any errors are detected. Configure an evaluation period, dimensions for each Lambda function and version, and the namespace as AWS/Lambda on the Errors metric.

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331
A DevOps engineer is deploying a new version of a companyâ€™s application in an AWS CodeDeploy deployment group associated with its Amazon EC2 instances. After some time, the deployment fails. The engineer realizes that all the events associated with the specific deployment ID are in a Skipped status, and code was not deployed in the instances associated with the deployment group.What are valid reasons for this failure? (Choose two.)

A. The networking configuration does not allow the EC2 instances to reach the internet via a NAT gateway or internet gateway, and the CodeDeploy endpoint cannot be reached.
B. The IAM user who triggered the application deployment does not have permission to interact with the CodeDeploy endpoint.
C. The target EC2 instances were not properly registered with the CodeDeploy endpoint.
D. An instance profile with proper permissions was not attached to the target EC2 instances.
E. The appspec.yml file was not included in the application revision.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
A company has a guideline that every Amazon EC2 instance must be launched from an AMI that the companyâ€™s security team produces. Every month, the security team sends an email message with the latest approved AMIs to all the development teams.The development teams use AWS CloudFormation to deploy their applications. When developers launch a new service, they have to search their email for the latest AMIs that the security department sent. A DevOps engineer wants to automate the process that the security team uses to provide the AMI IDs to the development teams.What is the MOST scalable solution that meets these requirements?

A. Direct the security team to use CloudFormation to create new versions of the AMIs and to list the AMI ARNs in an encrypted Amazon S3 object as part of the stackâ€™s Outputs section. Instruct the developers to use a cross-stack reference to load the encrypted S3 object and obtain the most recent AMI ARNs.
B. Direct the security team to use a CloudFormation stack to create an AWS CodePipeline pipeline that builds new AMIs and places the latest AMI ARNs in an encrypted Amazon S3 object as part of the pipeline output. Instruct the developers to use a cross-stack reference within their own CloudFormation template to obtain the S3 object location and the most recent AMI ARNs.
C. Direct the security team to use Amazon EC2 Image Builder to create new AMIs and to place the AMI ARNs as parameters in AWS Systems Manager Parameter Store. Instruct the developers to specify a parameter of type SSM in their CloudFormation stack to obtain the most recent AMI ARNs from Parameter Store.
D. Direct the security team to use Amazon EC2 Image Builder to create new AMIs and to create an Amazon Simple Notification Service (Amazon SNS) topic so that every development team can receive notifications. When the development teams receive a notification, instruct them to write an AWS Lambda function that will update their CloudFormation stack with the most recent AMI ARNs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 333
An application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). A DevOps engineer is using AWS CodeDeploy to release a new version. The deployment fails during the AllowTraffic lifecycle event, but a cause for the failure is not indicated in the deployment logs.What would cause this?

A. The appspec.yml file contains an invalid script that runs in the AllowTraffic lifecycle hook.
B. The user who initiated the deployment does not have the necessary permissions to interact with the AL
C. The health checks specified for the ALB target group are misconfigured.
D. The CodeDeploy agent was not installed in the EC2 instances that are part of the ALB target group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
A company has 20 service teams. Each service team is responsible for its own microservice. Each service team uses a separate AWS account for its microservice and a VPC with the 192.168.0.0/22 CIDR block. The company manages the AWS accounts with AWS Organizations.Each service team hosts its microservice on multiple Amazon EC2 instances behind an Application Load Balancer. The microservices communicate with each other across the public internet. The companyâ€™s security team has issued a new guideline that all communication between microservices must use HTTPS over private network connections and cannot traverse the public internet.A DevOps engineer must implement a solution that fulfills these obligations and minimizes the number of changes for each service team.Which solution will meet these requirements?

A. Create a new AWS account in AWS Organizations. Create a VPC in this account, and use AWS Resource Access Manager to share the private subnets of this VPC with the organization. Instruct the service teams to launch a new Network Load Balancer (NLB) and EC2 instances that use the shared private subnets. Use the NLB DNS names for communication between microservices.
B. Create a Network Load Balancer (NLB) in each of the microservice VPCs. Use AWS PrivateLink to create VPC endpoints in each AWS account for the NLBs. Create subscriptions to each VPC endpoint in each of the other AWS accounts. Use the VPC endpoint DNS names for communication between microservices.
C. Create a Network Load Balancer (NLB) in each of the microservice VPCs. Create VPC peering connections between each of the microservice VPCs. Update the route tables for each VPC to use the peering links. Use the NLB DNS names for communication between microservices.
D. Create a new AWS account in AWS Organizations. Create a transit gateway in this account, and use AWS Resource Access Manager to share the transit gateway with the organization. In each of the microservice VPCs, create a transit gateway attachment to the shared transit gateway. Update the route tables of each VPC to use the transit gateway. Create a Network Load Balancer (NLB) in each of the microservice VPCs. Use the NLB DNS names for communication between microservices.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335
An Amazon EC2 instance is running in a VPC and needs to download an object from a restricted Amazon S3 bucket. When the DevOps engineer tries to download the object, an AccessDenied error is received.What are

the possible causes for this error? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
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 fileâ€™s most recent members. Upload the new file to the S3 bucket.
D. Create a user data script that lists all members of the current security group of the cluster and automatically updates the /etc/cluster/nodes.config file whenever a new instance is added to the cluster.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337
A DevOps engineer is working on a data archival project that requires the migration of on-premises data to an Amazon S3 bucket. The DevOps engineer develops a script that incrementally archives on-premises data that is older than 1 month to Amazon S3. Data that is transferred to Amazon S3 is deleted from the on-premises location. The script uses the S3 PutObject operation.During a code review, the DevOps engineer notices that the script does not verify whether the data was successfully copied to Amazon S3. The DevOps engineer must update the script to ensure that data is not corrupted during transmission. The script must use MD5 checksums to verify data integrity before the on-premises data is deleted.Which solutions for the script will meet these requirements? (Choose two.)

A. Check the returned response for the VersionId. Compare the returned VersionId against the MD5 checksum.
B. Include the MD5 checksum within the Content-MD5 parameter. Check the operation callâ€™s return status

to find out if an error was returned.

C. Include the checksum digest within the tagging parameter as a URL query parameter.

D. Check the returned response for the ETag. Compare the returned ETag against the MD5 checksum.

E. Include the checksum digest within the Metadata parameter as a name-value pair. After upload, use the S3 HeadObject operation to retrieve metadata from the object.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338
A company uses AWS Key Management Service (AWS KMS) keys and manual key rotation to meet regulatory compliance requirements. The security team wants to be notified when any keys have not been rotated after 90 days.Which solution will accomplish this?

A. Configure AWS KMS to publish to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

B. Configure an Amazon EventBridge event to launch an AWS Lambda function to call the AWS Trusted Advisor API and publish to an Amazon Simple Notification Service (Amazon SNS) topic.

C. Develop an AWS Config custom rule that publishes to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

D. Configure AWS Security Hub to publish to an Amazon Simple Notification Service (Amazon SNS) topic when keys are more than 90 days old.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
A company deploys updates to its Amazon API Gateway API several times a week by using an AWS CodePipeline pipeline. As part of the update process, the company exports the JavaScript SDK for the API from the API Gateway console and uploads the SDK to an Amazon S3 bucket.The company has configured an Amazon CloudFront distribution that uses the S3 bucket as an origin. Web clients then download the SDK by using the CloudFront distributionâ€™s endpoint. A DevOps engineer needs to implement a solution to make the new SDK available automatically during new API deployments.Which solution will meet these requirements?

A. Create a CodePipeline action immediately after the deployment stage of the AP

B. Create a CodePipeline action immediately after the deployment stage of the AP

C. Create an Amazon EventBridge rule that reacts to UpdateStage events from aws.apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket, and call the CloudFront API to create an invalidation for the SDK path.

D. Create an Amazon EventBridge rule that reacts to CreateDeployment events from aws.apigateway. Configure the rule to invoke an AWS Lambda function to download the SDK from API Gateway, upload the SDK to the S3 bucket, and call the S3 API to invalidate the cache for the SDK path.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
A company has developed an AWS Lambda function that handles orders received through an API. The company is using AWS CodeDeploy to deploy the Lambda function as the final stage of a CI/CD pipeline.A DevOps engineer has noticed there are intermittent failures of the ordering API for a few seconds after deployment. After some investigation, the DevOps engineer believes the failures are due to database changes not having fully propagated before the Lambda function is invoked.How should the DevOps engineer overcome this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341
A company uses a single AWS account to test applications on Amazon EC2 instances. The company has turned on AWS Config in the AWS account and has activated the restricted-ssh AWS Config managed rule.The company needs an automated monitoring solution that will provide a customized notification in real time if any security group in the account is not compliant with the restricted-ssh rule. The customized notification must contain the name and ID of the noncompliant security group.A DevOps engineer creates an Amazon Simple Notification Service (Amazon SNS) topic in the account and subscribes the appropriate personnel to the topic.What should the DevOps engineer do next to meet these requirements?

A. Create an Amazon EventBridge rule that matches an AWS Config evaluation result of NON_COMPLIANT for the restricted-ssh rule. Configure an input transformer for the EventBridge rule. Configure the EventBridge rule to publish a notification to the SNS topic.
B. Configure AWS Config to send all evaluation results for the restricted-ssh rule to the SNS topic. Configure a filter policy on the SNS topic to send only notifications that contain the text of NON_COMPLIANT in the notification to subscribers.
C. Create an Amazon EventBridge rule that matches an AWS Config evaluation result of NON_COMPLIANT for the restricted-ssh rule. Configure the EventBridge rule to invoke AWS Systems Manager Run Command on the SNS topic to customize a notification and to publish the notification to the SNS topic.
D. Create an Amazon EventBridge rule that matches all AWS Config evaluation results of NON_COMPLIAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
A company requires an RPO of 2 hours and an RTO of 10 minutes for its data and application at all times. An application uses a MySQL database and Amazon EC2 web servers. The development team needs a strategy

for failover and disaster recovery.Which combination of deployment strategies will meet these requirements? (Choose two.)

A. Create an Amazon Aurora cluster in one Availability Zone across multiple Regions as the data store. Use Auroraâ€™s automatic recovery capabilities in the event of a disaster.
B. Create an Amazon Aurora global database in two Regions as the data store. In the event of a failure, promote the secondary Region as the primary for the application.
C. Create an Amazon Aurora multi-master cluster across multiple Regions as the data store. Use a Network Load Balancer to balance the database traffic in different Regions.
D. Set up the application in two Regions and use Amazon Route 53 failover-based routing that points to the Application Load Balancers in both Regions. Use health checks to determine the availability in a given Region. Use Auto Scaling groups in each Region to adjust capacity based on demand.
E. Set up the application in two Regions and use a multi-Region Auto Scaling group behind Application Load Balancers to manage the capacity based on demand. In the event of a disaster, adjust the Auto Scaling groupâ€™s desired instance count to increase baseline capacity in the failover Region.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343
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 EventBridge rule to ensure the pipeline 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 run actions for each Lambda function in parallel by specifying the same runOrder.
D. Modify each CodeBuild project to run within a VPC and use dedicated instances to increase throughput.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 344
A company uses AWS CloudFormation stacks to deploy updates to its application. The stacks consist of different resources. The resources include AWS Auto Scaling groups, Amazon EC2 instances, Application Load Balancers (ALBs), and other resources that are necessary to launch and maintain independent stacks. Changes to application resources outside of CloudFormation stack updates are not allowed.The company recently attempted to update the application stack by using the AWS CLI. The stack failed to update and produced the following error message: â€œERROR: both the deployment and the CloudFormation stack rollback failed. The deployment failed because the following resource(s) failed to update: [AutoScalingGroup].â€The stack remains in a status of UPDATE_ROLLBACK_FAILED.Which solution will resolve this issue?

A. Update the subnet mappings that are configured for the ALBs. Run the aws cloudformation update-stack-

set AWS CLI command.

B. Update the IAM role by providing the necessary permissions to update the stack. Run the aws cloudformation continue-update-rollback AWS CLI command.

C. Submit a request for a quota increase for the number of EC2 instances for the account. Run the aws cloudformation cancel-update-stack AWS CLI command.

D. Delete the Auto Scaling group resource. Run the aws cloudformation rollback-stack AWS CLI command.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
A company is deploying a new application that uses Amazon EC2 instances. The company needs a solution to query application logs and AWS account API activity.Which solution will meet these requirements?

A. Use the Amazon CloudWatch agent to send logs from the EC2 instances to Amazon CloudWatch Logs. Configure AWS CloudTrail to deliver the API logs to Amazon S3. Use CloudWatch to query both sets of logs.

B. Use the Amazon CloudWatch agent to send logs from the EC2 instances to Amazon CloudWatch Logs. Configure AWS CloudTrail to deliver the API logs to CloudWatch Logs. Use CloudWatch Logs Insights to query both sets of logs.

C. Use the Amazon CloudWatch agent to send logs from the EC2 instances to Amazon Kinesis. Configure AWS CloudTrail to deliver the API logs to Kinesis. Use Kinesis to load the data into Amazon Redshift. Use Amazon Redshift to query both sets of logs.

D. Use the Amazon CloudWatch agent to send logs from the EC2 instances to Amazon S3. Use AWS CloudTrail to deliver the API logs to Amazon S3. Use Amazon Athena to query both sets of logs in Amazon S3.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
A company wants to ensure that their EC2 instances are secure. They want to be notified if any new vulnerabilities are discovered on their instances, and they also want an audit trail of all login activities on the instances.Which solution will meet these requirements?

A. Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Amazon Kinesis Agent to capture system logs and deliver them to Amazon S3.

B. Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Systems Manager Agent to capture system logs and view login activity in the CloudTrail console.

C. Configure Amazon CloudWatch to detect vulnerabilities on the EC2 instances. Install the AWS Config daemon to capture system logs and view them in the AWS Config console.

D. Configure Amazon Inspector to detect vulnerabilities on the EC2 instances. Install the Amazon CloudWatch Agent to capture system logs and record them via Amazon CloudWatch Logs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 347
A company is running an application on Amazon EC2 instances in an Auto Scaling group. Recently, an issue occurred that prevented EC2 instances from launching successfully, and it took several hours for the support team to discover the issue. The support team wants to be notified by email whenever an EC2 instance does not start successfully.Which action will accomplish this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 348
A company is using AWS Organizations to centrally manage its AWS accounts. The company has turned on AWS Config in each member account by using AWS CloudFormation StackSets. The company has configured trusted access in Organizations for AWS Config and has configured a member account as a delegated administrator account for AWS Config.A DevOps engineer needs to implement a new security policy. The policy must require all current and future AWS member accounts to use a common baseline of AWS Config rules that contain remediation actions that are managed from a central account. Non-administrator users who can access member accounts must not be able to modify this common baseline of AWS Config rules that are deployed into each member account.Which solution will meet these requirements?

A. Create a CloudFormation template that contains the AWS Config rules and remediation actions. Deploy the template from the Organizations management account by using CloudFormation StackSets.
B. Create an AWS Config conformance pack that contains the AWS Config rules and remediation actions. Deploy the pack from the Organizations management account by using CloudFormation StackSets.
C. Create a CloudFormation template that contains the AWS Config rules and remediation actions. Deploy the template from the delegated administrator account by using AWS Config.
D. Create an AWS Config conformance pack that contains the AWS Config rules and remediation actions. Deploy the pack from the delegated administrator account by using AWS Config.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: