QUESTION 967
A company runs a multi-tier web application with two Amazon EC2 instances in one Availability Zone in the us-east-1 Region. A SysOps administrator must migrate one of the EC2 instances to a new Availability Zone.
Which solution will accomplish this?

A. Copy the EC2 instance to a different Availability Zone.
Terminate the original instance.
B. Create an Amazon Machine Image (AMI) from the EC2 instance and launch it in a different Availability Zone.
Terminate the original instance.
C. Move the EC2 instance to a different Availability Zone using the AWS CLI.
D. Stop the EC2 instance, modify the Availability Zone, and start the instance.

Answer: B

QUESTION 968
A company's application infrastructure was deployed using AWS CloudFormation and is composed of Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones. When releasing a new version of the application, the update deployment must avoid DNS changes and allow rollback.
Which solution should a SysOps administrator use to meet the deployment requirements for this new release?

A. Configure the Auto Scaling group to use lifecycle hooks.
Deploy new instances with the new application version.
Complete the lifecycle hook action once healthy.
B. Create a new Amazon Machine Image (AMI) containing the updated code.
Create a launch configuration with the AMI.
Update the Auto Scaling group to use the new launch configuration.
C. Deploy a second CloudFormation stack. Wait for the application to be available.
Cut over to the new Application Load Balancer.
D. Modify the CloudFormation template to use an AutoScalingReplacingUpdate policy.
Update the stack.
Perform a second update with the new release.

Answer: A

QUESTION 969
A company wants to launch a group of Amazon EC2 instances that need to communicate with each other with the lowest possible latency.
Which combination of actions should a SysOps administrator take when launching these instances? (Choose two.)

A. Launch instances in different VPCs with a VPN tunnel.
B. Launch instances in different VPCs with VPC peering enabled.
C. Launch instances in a cluster placement group.
D. Launch instances in a spread placement group.
E. Launch instances with enhanced networking enabled.

Answer: CE

QUESTION 970
A company has multiple AWS accounts. The company uses AWS Organizations with an organizational unit (OU) for the production account and another OU for the development account. Corporate policies state that developers may use only approved AWS services in the production account.
What is the MOST operationally efficient solution to control the production account?

A. Create a customer managed policy in AWS Identity and Access Management (IAM).
Apply the policy to all users within the production account.
B. Create a job function policy in AWS Identity and Access Management (IAM).
Apply the policy to all users within the production OU.
C. Create a service control policy (SCP).
Apply the SCP to the production OU.
D. Create an IAM policy.
Apply the policy in Amazon API Gateway to restrict the production account.

Answer: A

QUESTION 971
A company's data processing workflow uses AWS Lambda to interact with other AWS services, including AWS Step Functions, Amazon DynamoDB, and Amazon S3. The Lambda functions make several API calls to these services as a part of the workflow. AWS CloudTrail has been enabled in the AWS Region and is logging to Amazon CloudWatch Logs. The Lambda functions are also logging to CloudWatch Logs.
A SysOps administrator notices that a specific Lambda function in the workflow is taking longer to run than it did last month. The SysOps administrator needs to determine the parts of the Lambda function that are experiencing higher-than-normal response times.
What solution will accomplish this?

A. Analyze logs in CloudWatch Logs for the timestamps at which the API calls are made while the Lambda function is running.
Compare with the logs from the previous month.
B. Enable AWS X-Ray for the function.
Analyze the service map and traces to help identify the API calls with anomalous response times.
C. Search CloudTrail logs for the calls from the Lambda function.
Compare the observed and expected times of API calls relative to the time when the function starts.
D. Use CloudWatch to monitor the Duration metric of function invocations for the Lambda function.
Compare with the measurements from the previous month.

Answer: D

QUESTION 972
Developers are using IAM access keys to manage AWS resources using AWS CLI. Company policy requires that access keys are automatically disabled when the access key age is greater than 90 days.
Which solution will accomplish this?

A. Configure an Amazon CloudWatch alarm to trigger an AWS Lambda function that disables keys older than 90 days.

B. Configure AWS Trusted Advisor to identify and disable keys older than 90 days.
C. Set a password policy on the account with a 90-day expiration.
D. Use an AWS Config rule to identify noncompliant keys.
Create a custom AWS Systems Manager Automation document for remediation.

Answer: D

QUESTION 973
A company wants to store sensitive data in Amazon S3. The S3 bucket and its contents must be accessible only from the on-premises corporate network.
What should a SysOps administrator do to configure the S3 bucket policy statement?

A. Use a Deny effect with a condition based on the aws:sourceVpc key.
B. Use a Deny effect with a condition based on the NotIpAddress key.
C. Use an Allow effect with a condition based on the IpAddress key.
D. Use an Allow effect with a condition based on the s3:LocationConstraint key.

Answer: A

QUESTION 974
A SysOps administrator wants to encrypt an existing Amazon RDS DB instance with AWS Key Management Service (AWS KMS).
How should the SysOps administrator accomplish this goal?

A. Copy the data volumes of the unencrypted instance.
Apply the KMS key to the copied data volumes.
Start the instance with the encrypted volumes.
B. Create a read replica of the unencrypted instance.
Encrypt the read replica with the KMS key.
Promote the read replica to become the primary instance.
C. Take a snapshot of the unencrypted instance.
Apply the KMS key to the existing instance using the modify-db-instance command. Restart the instance.
D. Take a snapshot of the unencrypted instance.
Create an encrypted copy of the snapshot with the KMS key.
Restore the instance from the encrypted snapshot.

Answer: A

QUESTION 975
A company needs to deploy a web application on two Amazon EC2 instances behind an Application Load Balancer (ALB). Two EC2 instances will also be deployed to host the database. The infrastructure needs to be designed across Availability Zones (AZs) for high availability and must limit public access to the instances as much as possible.
How should this be achieved within a VPC?

A. Use two AZs and create a public subnet in each AZ for the Application Load Balancer, a private subnet in each AZ for the web servers, and a private subnet in each AZ for the database servers.
B. Use two AZs and create a public subnet in each AZ for the Application Load Balancer, a public subnet in each AZ for the web servers, and a public subnet in each AZ for the database servers.
C. Use two AZs and create one public subnet for the Application Load Balancer, a private subnet in each AZ for the web servers, and a public subnet in each AZ for the database servers.
D. Use two AZs and create one public subnet for the Application Load Balancer, a public subnet in each AZ for the web servers, and a private subnet in each AZ for the database servers.

Answer: A

QUESTION 976
A SysOps administrator is responsible for managing a fleet of Amazon EC2 instances. These EC2 instances upload build artifacts to a third-party service. The third-party service recently implemented strict IP whitelisting that requires all build uploads to come from a single IP address.
What change should the systems administrator make to the existing build fleet to comply with this new requirement?

A. Move all of the EC2 instances behind a NAT gateway and provide the gateway IP address to the service.
B. Move all of the EC2 instances behind an internet gateway and provide the gateway IP address to the service.
C. Move all of the EC2 instances into a single Availability Zone and provide the Availability Zone IP address to the service.
D. Move all of the EC2 instances to a peered VPC and provide the VPC IP address to the service.

Answer: C

QUESTION 977
A SysOps administrator manages an AWS CloudFormation template that provisions Amazon EC2 instances, an Elastic Load Balancer, and Amazon RDS instances. As part of an ongoing transformation project, CloudFormation stacks are being created and deleted continuously. The administrator needs to ensure that the RDS instances continue running after a stack has been deleted.
Which action should be taken to meet these requirements?

A. Edit the template to remove the RDS resources and update the stack.
B. Enable termination protection on the stack.
C. Set the DeletionPolicy attribute for RDS resources to Retain in the template.
D. Set the deletion-protection parameter on RDS resources.

Answer: C

QUESTION 978
A streaming company is using AWS resources in the us-east-1 Region for its production environment. The web tier of the streaming site 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 Auto Scaling group is configured to scale when the CPU utilization of the instances is greater than 75%. The user database is hosted on an Amazon RDS MySQL cluster, and video content is stored within an Amazon S3 bucket. Amazon CloudWatch metrics show that the RDS MySQL Multi-AZ DB instance has around 16 GB of memory free and an average CPU utilization of 70%. It is taking users in Asia several seconds longer to access the streaming website.
Which combination of actions will improve the access load times? (Choose two.)

A. Configure RDS MySQL Multi-AZ to reduce RDS CPU and RAM utilization and distribute queries to multiple Availability Zones.
B. Modify the EC2 Auto Scaling group so it will scale horizontally when CPU utilization is 50%.
C. Provision a second production environment in the Asia Pacific Region and use an ALB to distribute cross-Region access.
D. Provision a second production environment in the Asia Pacific Region and use Amazon Route 53 latency-based routing.
E. Set up an Amazon CloudFront distribution to handle static content for users accessing it from different geographic locations.

Answer: BC

QUESTION 979
A large company has multiple AWS accounts that are assigned to each department. A SysOps administrator needs to help the company reduce overhead and manage its AWS resources more easily. The SysOps administrator also must ensure that department users, including AWS account root users, have access only to AWS services that are essential for their job function.

Which solution will meet these requirements?

A. Enable AWS Directory Service.
Enforce Group Policy Objects (GPOs) on each department to restrict access.
B. Migrate all the accounts to a central account.
Create IAM groups for each department with only the necessary permissions.
C. Use AWS Organizations and implement service control policies (SCPs) to ensure accounts use only essential AWS services.
D. Use AWS Single Sign-On and configure it to limit access to only essential AWS services.

Answer: A

QUESTION 980
A security officer has requested that internet access be removed from subnets in a VPC. The subnets currently route internet-bound traffic to a NAT gateway. A SysOps administrator needs to remove this access while allowing access to Amazon S3.
Which solution will meet these requirements?

A. Set up an internet gateway.
Update the route table on the subnets to use the internet gateway to route traffic to Amazon S3.
B. Set up an S3 VPC gateway endpoint.
Update the route table on the subnets to use the gateway endpoint to route traffic to Amazon S3.
C. Set up additional NAT gateways in each Availability Zone.
Update the route table on the subnets to use the NAT gateways to route traffic to Amazon S3.
D. Set up an egress-only internet gateway.
Update the route table on the subnets to use the egress-only internet gateway to route traffic to Amazon S3.

Answer: C

QUESTION 981
An application is running on Amazon EC2 instances and storing all application data in Amazon S3. The company wants to archive all files older than 30 days to reduce costs. Archived files are used for auditing purposes only; however, the audit team may need to retrieve files in under a minute.
How should the SysOps administrator implement these requirements?

A. Configure an S3 bucket policy to move all objects older than 30 days to S3 Standard-Infrequent Access (S3 Standard-IA).
B. Create a lifecycle rule to move all objects older than 30 days to S3 Glacier.
C. Create a lifecycle rule to move all objects older than 30 days to S3 Standard-Infrequent Access (S3 Standard-IA).
D. Use S3 Intelligent-Tiering to move files older than 30 days to S3 Glacier Deep Archive.

Answer: A

QUESTION 982
A company has developed a new memory-intensive application that is deployed to a large Amazon EC2 Linux fleet. The company is concerned about potential memory exhaustion, so the development team wants to monitor memory usage by using Amazon CloudWatch.
What is the MOST operationally efficient way to accomplish this goal?

A. Create an AWS Lambda function to capture memory utilization of the EC2 instances.
Schedule the Lambda function with Amazon EventBridge (Amazon CloudWatch Events).
B. Deploy the application to memory optimized EC2 instances.
Use the CloudWatch MemoryUtilization metric.
C. Install the CloudWatch agent on the EC2 instances to collect and send metrics to CloudWatch.

D. Install the CloudWatch monitoring scripts on the EC2 instances to collect and send metrics to CloudWatch.

Answer: D

QUESTION 983
A company uses LDAP-based credentials and has a Security Assertion Markup Language (SAML) 2.0 identity provider. A SysOps administrator has configured various federated roles in a new AWS account to provide AWS Management Console access for groups of users that use the existing LDAP-based credentials. Several groups want to use the AWS CLI on their workstations to automate daily tasks. To enable them to do so, the SysOps administrator has created an application that authenticates a user and generates a SAML assertion
Which API call should be used to retrieve credentials for federated programmatic access?

A. sts:AssumeRole
B. sts:AssumeRoleWithSAML
C. sts:AssumeRoleWithWebIdentity
D. sts:GetFederationToken

Answer: B