AWS SysOps Administrator Associate Certification Example Questions

1) A company hosts a web application on an Amazon EC2 instance. Users report that the web application is occasionally unresponsive. Amazon CloudWatch metrics indicate that the CPU utilization is 100% during these times. A SysOps administrator must implement a solution to monitor for this issue. Which solution will meet this requirement?

A. Create a CloudWatch alarm that monitors AWS CloudTrail events for the EC2 instance.

B. Create a CloudWatch alarm that monitors CloudWatch metrics for EC2 instance CPU utilization.

C. Create an Amazon Simple Notification Service (Amazon SNS) topic to monitor CloudWatch metrics for EC2 instance CPU utilization.

D. Create a recurring assessment check on the EC2 instance by using Amazon Inspector to detect deviations in CPU utilization.

2) A company has an application that uses Amazon ElastiCache for Memcached to cache query responses to improve latency. However, the application's users are reporting slow response times. A SysOps administrator notices that the Amazon CloudWatch metrics for Memcached evictions are high. Which actions should the SysOps administrator take to fix this issue? (Select two choices)

A. Flush the contents of ElastiCache for Memcached.

B. Increase the ConnectionOverhead parameter value.

C. Increase the number of nodes in the cluster.

D. Increase the size of the nodes in the cluster.

E. Decrease the number of nodes in the cluster.

3) A company needs to ensure that an AWS Lambda function can access resources in a VPC in the company's account. The Lambda function requires access to third-party APIs that can be accessed only over the internet. Which action should a SysOps administrator take to meet these requirements?

A. Attach an Elastic IP address to the Lambda function and configure a route to the internet gateway of the VPC.

B. Connect the Lambda function to a private subnet that has a route to the virtual private gateway of the VPC.

C. Connect the Lambda function to a public subnet that has a route to the internet gateway of the VPC.

D. Connect the Lambda function to a private subnet that has a route to a NAT gateway deployed in a public subnet of the VPC.

4) A company runs an application on a large fleet of Amazon EC2 instances to process financial transactions. The EC2 instances share data by using an Amazon Elastic File System (Amazon EFS) file system. The company wants to deploy the application to a new Availability Zone and has created new subnets and a mount target in the new Availability Zone. When a SysOps administrator launches new EC2 instances in the new subnets, the EC2 instances are unable to mount the file system. What is a reason for this issue?

A. The EFS mount target has been created in a private subnet.

B. The IAM role that is associated with the EC2 instances does not allow the efs:MountFileSystem action.

C. The route tables have not been configured to route traffic to a VPC endpoint for Amazon EFS in the new Availability Zone.

D. The security group for the mount target does not allow inbound NFS connections from the security group used by the EC2 instances.

5) A company uses AWS Organizations to create and manage many AWS accounts. The company wants to deploy new IAM roles in each account. Which action should the SysOps administrator take to deploy the new roles in each of the organization's accounts?

A. Create a service control policy (SCP) in the organization to add the new IAM roles to each account.

B. Deploy an AWS CloudFormation change set to the organization with a template to create the new IAM roles.

C. Use AWS CloudFormation StackSets to deploy a template to each account to create the new IAM roles.

D. Use AWS Config to create an organization rule to add the new IAM roles to each account.

6) A company runs several production workloads on Amazon EC2 instances. A SysOps administrator discovered that a production EC2 instance failed a system health check. The SysOps administrator recovered the instance manually. The SysOps administrator wants to automate the recovery task of EC2 instances and receive notifications whenever a system health check fails. Detailed monitoring is activated for all of the company's production EC2 instances. Which of the following is the MOST operationally efficient solution that meets these requirements?

A. For each production EC2 instance, create an Amazon CloudWatch alarm for Status Check Failed: System. Set the alarm action to recover the EC2 instance. Configure the alarm notification to be published to an Amazon Simple Notification Service (Amazon SNS) topic.

B. On each production EC2 instance, create a script that monitors the system health by sending a heartbeat notification every minute to a central monitoring server. If an EC2 instance fails to send a heartbeat, run a script on the monitoring server to stop and start the EC2 instance and to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.

C. On each production EC2 instance, create a script that sends network pings to a highly available endpoint by way of a cron job. If the script detects a network response timeout, invoke a command to reboot the EC2 instance.

D. On each production EC2 instance, configure an Amazon CloudWatch agent to collect and send logs to a log group in Amazon CloudWatch Logs. Create a CloudWatch alarm that is based on a metric filter that tracks errors. Configure the alarm to invoke an AWS Lambda function to reboot the EC2 instance and send a notification email.

7) The company uses AWS Organizations to manage its accounts. For the production account, a SysOps administrator must ensure that all data is backed up daily for all current and future Amazon EC2 instances and Amazon Elastic File System (Amazon EFS) file systems. Backups must be retained for 30 days. Which solution will meet these requirements with the LEAST amount of effort?

A. Create a backup plan in AWS Backup. Assign resources by resource ID, selecting all existing EC2 and EFS resources that are running in the account. Edit the backup plan daily to include any new resources. Schedule the backup plan to run every day with a lifecycle policy to expire backups after 30 days.

B. Create a backup plan in AWS Backup. Assign resources by tags. Ensure that all existing EC2 and EFS resources are tagged correctly. Apply a service control policy (SCP) for the production account OU that prevents instance and file system creation unless the correct tags are applied. Schedule the backup plan to run every day with a lifecycle policy to expire backups after 30 days.

C. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by resource ID, selecting all existing EC2 and EFS resources that are running in the account. Edit the lifecycle policy daily to include any new resources. Schedule the lifecycle policy to create snapshots every day with a retention period of 30 days.

D. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by tags. Ensure that all existing EC2 and EFS resources are tagged correctly. Apply a service control policy (SCP) that prevents resource creation unless the correct tags are applied. Schedule the lifecycle policy to create snapshots every day with a retention period of 30 days

8) A company is using AWS CloudTrail and wants to ensure that SysOps administrators can easily verify that the log files have not been deleted or changed. Which action should a SysOps administrator take to meet this requirement?

A. Grant administrators access to the AWS Key Management Service (AWS KMS) key used to encrypt the log files.

B. Enable CloudTrail log file integrity validation when the trail is created or updated.

C. Turn on Amazon S3 server access logging for the bucket storing the log files.

D. Configure the S3 bucket to replicate the log files to another bucket.

9) A company is running a custom database on an Amazon EC2 instance. The database stores its data on an Amazon Elastic Block Store (Amazon EBS) volume.
A SysOps administrator must set up a backup strategy for the EBS volume. What should the SysOps administrator do to meet this requirement?

A. Create an Amazon CloudWatch alarm for the VolumeIdleTime metric with an action to take a snapshot of the EBS volume.

B. Create a pipeline in AWS Data Pipeline to take a snapshot of the EBS volume on a recurring schedule.

C. Create an Amazon Data Lifecycle Manager (Amazon DLM) policy to take a snapshot of the EBS volume on a recurring schedule.

D. Create an AWS DataSync task to take a snapshot of the EBS volume on a recurring schedule.

10) A company runs a large number of Amazon EC2 instances for internal departments. The company needs to track the costs of its existing AWS resources by the department. What should a SysOps administrator do to meet this requirement?

A. Activate all of the AWS-generated cost allocation tags for the account.

B. Apply user-defined tags to the instances through Tag Editor. Activate these tags for cost allocation.

C. Schedule an AWS Lambda function to run the AWS Pricing Calculator for EC2 usage on a recurring schedule.

D. Use the AWS Trusted Advisor dashboard to export EC2 cost reports.

Answers

1) B

2) C, D

3) D

4) D

5) C

6) A

7) B

8) B

9) C

10) B