

Exam : DOP-C01

**Title : AWS DevOps Engineer -
Professional**

Version : DEMO

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

Which changes should a DevOps Engineer make to the test and deployment process? (Choose two.)

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

Answer: D,E

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

What should a DevOps engineer do to meet these requirements?

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

Answer: B

3.A DevOps Engineer is leading the implementation for automating patching of Windows-based workstations in a hybrid cloud environment by using AWS Systems Manager (SSM).

What steps should the Engineer follow to set up Systems Manager to automate patching in this environment? (Select TWO.)

- A. Create multiple IAM service roles for Systems Manager so that the ssm.amazonaws.com service can execute the AssumeRole operation on every instance. Register the role on a per-resource level to enable the creation of a service token. Perform managed-instance activation with the newly created service role attached to each managed instance.
- B. Create an IAM service role for Systems Manager so that the ssm.amazonaws.com service can execute the AssumeRole operation. Register the role to enable the creation of a service token. Perform managed-instance activation with the newly created service role.
- C. Using previously obtained activation codes and activation IDs, download and install the SSM Agent on

the hybrid servers, and register the servers or virtual machines on the Systems Manager service. Hybrid instances will show with an "mi-" prefix in the SSM console.

D. Using previously obtained activation codes and activation IDs, download and install the SSM Agent on the hybrid servers, and register the servers or virtual machines on the Systems Manager service. Hybrid instances will show with an "i-" prefix in the SSM console as if they were provisioned as a regular Amazon EC2 instance.

E. Run AWS Config to create a list of instances that are unpatched and not compliant. Create an instance scheduler job, and through an AWS Lambda function, perform the instance patching to bring them up to compliance.

Answer: B,C

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-managed-instance-activation.html>

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-managed-win.html>

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

A. Auto Scaling groups can create new instances in a single AZ only.

B. The EC2 instances have not been manually associated to the ALB.

C. The ALB should be replaced with a Network Load Balancer (NLB).

D. The new AZ has not been added to the ALB.

Answer: D

5. You have an application running a specific process that is critical to the application's functionality, and have added the health check process to your Auto Scaling Group. The instances are showing healthy but the application itself is not working as it should.

What could be the issue with the health check, since it is still showing the instances as healthy?

A. You do not have the time range in the health check properly configured.

B. It is not possible for a health check to monitor a process that involves the application.

C. The health check is not configured properly.

D. The health check is not checking the application process.

Answer: D

Explanation:

If you have custom health checks, you can send the information from your health checks to Auto Scaling so that Auto Scaling can use this information. For example, if you determine that an instance is not functioning as expected, you can set the health status of the instance to Unhealthy.

The next time that Auto Scaling performs a health check on the instance, it will determine that the instance is unhealthy and then launch a replacement instance.

For more information on Autoscaling health checks, please refer to the below document link: from AWS

🔗 <http://docs.aws.amazon.com/autoscaling/latest/userguide/healthcheck.html>