



DOP-C01^{Q&As}

AWS Certified DevOps Engineer - Professional (DOP-C01)

Pass Amazon DOP-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/aws-devops-engineer-professional.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A DevOps Engineer encountered the following error when attempting to use an AWS CloudFormation template to create an Amazon ECS cluster:

An error occurred (InsufficientCapabilitiesException) when calling the CreateStack operation.

What caused this error and what steps need to be taken to allow the Engineer to successfully execute the AWS CloudFormation template?

- A. The AWS user or role attempting to execute the CloudFormation template does not have the permissions required to create the resources within the template. The Engineer must review the user policies and add any permissions needed to create the resources and then rerun the template execution.
- B. The AWS CloudFormation service cannot be reached and is not capable of creating the cluster. The Engineer needs to confirm that routing and firewall rules are not preventing the AWS CloudFormation script from communicating with the AWS service endpoints, and then rerun the template execution.
- C. The CloudFormation execution was not granted the capability to create IAM resources. The Engineer needs to provide CAPABILITY_IAM and CAPABILITY_NAMED_IAM as capabilities in the CloudFormation execution parameters or provide the capabilities in the AWS Management Console.
- D. CloudFormation is not capable of fulfilling the request of the specified resources in the current AWS Region. The Engineer needs to specify a new region and rerun the template.

Correct Answer: C

Reference: <https://github.com/aws-labs/serverless-application-model/issues/51>

QUESTION 2

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 (Amazon CloudWatch Events) event rule that is invoked by GuardDuty events that are CRITICAL. Define an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the security team's email address to the topic.



D. Use AWS Firewall Manager to apply consistent policies across all accounts. Create an Amazon EventBridge (Amazon CloudWatch Events) event rule that is invoked by Firewall Manager events that are CRITICAL. Define an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the security team's email address to the topic.

Correct Answer: C

QUESTION 3

A legacy web application stores access logs in a proprietary text format. One of the security requirements is to search application access events and correlate them with access data from many different systems.

These searches should be near-real time.

Which solution offloads the processing load on the application server and provides a mechanism to search the data in near-real time?

- A. Install the Amazon CloudWatch Logs agent on the application server and use CloudWatch Events rules to search logs for access events. Use Amazon CloudSearch as an interface to search for events.
- B. Use the third-party file-input plugin Logstash to monitor the application log file, then use a custom dissect filter on the agent to parse the log entries into the JSON format. Output the events to Amazon ES to be searched. Use the Elasticsearch API for querying the data.
- C. Upload the log files to Amazon S3 by using the S3 sync command. Use Amazon Athena to define the structure of the data as a table, with Athena SQL queries to search for access events.
- D. Install the Amazon Kinesis Agent on the application server, configure it to monitor the log files, and send it to a Kinesis stream. Configure Kinesis to transform the data by using an AWS Lambda function, and forward events to Amazon ES for analysis. Use the Elasticsearch API for querying the data.

Correct Answer: D

QUESTION 4

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: A

Reference: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-maintain-instance-levels.html>

QUESTION 5

On which local address does the Docker DNS server listen?

- A. 127.0.0.1
- B. 127.0.0.111
- C. 127.0.0.254
- D. 127.0.0.11

Correct Answer: D

Note: If you need access to a host's localhost resolver, you must modify your DNS service on the host to listen on a non-localhost address that is reachable from within the container. Note: The DNS server is always at 127.0.0.11.

Reference: <https://docs.docker.com/engine/userguide/networking/configure-dns/>

[Latest DOP-C01 Dumps](#)

[DOP-C01 Study Guide](#)

[DOP-C01 Braindumps](#)