



## Exam AWS Certified Developer - Associate DVA-C02 All Questions

View all questions & answers for the AWS Certified Developer - Associate DVA-C02 exam

[Go to Exam](#)

### EXAM AWS CERTIFIED DEVELOPER - ASSOCIATE DVA-C02 TOPIC 1 QUESTION 10 DISCU...

Exam question from Amazon's AWS Certified Developer - Associate DVA-C02

Question #: 10

Topic #: 1

[\[All AWS Certified Developer - Associate DVA-C02 Questions\]](#)

A developer is deploying a new application to Amazon Elastic Container Service (Amazon ECS). The developer needs to securely store and retrieve different types of variables. These variables include authentication information for a remote API, the URL for the API, and credentials. The authentication information and API URL must be available to all current and future deployed versions of the application across development, testing, and production environments.

How should the developer retrieve the variables with the FEWEST application changes?

- A. Update the application to retrieve the variables from AWS Systems Manager Parameter Store. Use unique paths in Parameter Store for each variable in each environment. Store the credentials in AWS Secrets Manager in each environment.
- B. Update the application to retrieve the variables from AWS Key Management Service (AWS KMS). Store the API URL and credentials as unique keys for each environment.
- C. Update the application to retrieve the variables from an encrypted file that is stored with the application. Store the API URL and credentials in unique files for each environment.
- D. Update the application to retrieve the variables from each of the deployed environments. Define the authentication information and API URL in the ECS task definition as unique names during the deployment process.

[Show Suggested Answer](#)

by [Warlord\\_92](#) at March 20, 2023, 7:24 a.m.

Disclaimers:

- ExamTopics website is **not** related to, affiliated with, endorsed or authorized by Amazon.
- Trademarks, certification & product names are used for reference only and belong to Amazon.

### Comments

 [geekdamsel](#) [Highly Voted](#) 2 years ago

Correct answer is A.

upvoted 18 times

 [Warlord\\_92](#) [Highly Voted](#) 2 years, 1 month ago

[Selected Answer: A](#)

The application has credentials and URL, so it's convenient to store them in ssm parameter store restive them.

upvoted 9 times


 [sumanshu](#) [Most Recent](#) 4 months, 4 weeks ago

[Selected Answer: A](#)

B) Eliminated - It cannot directly store variables such as the API URL or credentials


D) Eliminated - Storing sensitive information like credentials directly in ECS task definitions is not secure

upvoted 1 times

 [sumanshu](#) 4 months, 4 weeks ago

C) Eliminated - Storing variables in encrypted files adds operational overhead. Managing separate files for each environment can quickly become cumbersome.

upvoted 1 times

 [trieudo](#) 5 months, 1 week ago

[Selected Answer: A](#)

keyword: FEWEST application changes

==> A: This minimizes code changes as the retrieval method remains consistent across environments; only the Parameter Store paths need updating. Secrets Manager securely stores sensitive credentials.

upvoted 1 times

 [Tee400](#) 7 months, 3 weeks ago

[Selected Answer: A](#)

AWS Systems Manager Parameter Store is a service that allows you to securely store configuration data such as API URLs, credentials, and other variables. By updating the application to retrieve the variables from Parameter Store, you can separate the configuration from the application code, making it easier to manage and update the variables without modifying the application itself. Storing the credentials in AWS Secrets Manager provides an additional layer of security for sensitive information.

upvoted 2 times

 [badsati](#) 7 months, 3 weeks ago

Answer is A

AWS Systems Manager Parameter Store and AWS Secrets Manager are designed for securely storing and managing sensitive information such as credentials, API URLs, and configuration variables. Using AWS Systems Manager Parameter Store allows the developer to centrally manage configuration variables across different environments (development, testing, production) without requiring application code changes. Each variable can have a unique path in Parameter Store, ensuring separation and organization.

upvoted 2 times

🗨️ **ez\_24** 7 months, 3 weeks ago

Correct Answer is A

Option B, using AWS Key Management Service (AWS KMS), is not ideal for this scenario primarily because AWS KMS is designed for creating and controlling encryption keys, not for storing configuration data or credentials. KMS keys are used to encrypt and decrypt data, rather than directly storing or managing it. For securely managing and retrieving application configuration data and sensitive information like API credentials, Systems Manager Parameter Store and AWS Secrets Manager are more appropriate, offering direct support for these use cases with better integration for applications.

upvoted 5 times

🗨️ **65703c1** 12 months ago

**Selected Answer: A**

A is the correct answer.

upvoted 1 times

🗨️ **Prosen2522** 1 year ago

**Selected Answer: A**

SSM parameter store with proper posh is the answer.

upvoted 1 times

🗨️ **leonardoliveros** 1 year, 6 months ago

**Selected Answer: A**

You put the different variables for each environment, is the best solution because it's isolated between environment

upvoted 2 times

🗨️ **vmintam** 1 year, 6 months ago

i think corrent is A, but why is B ?

upvoted 2 times

🗨️ **alihaider907** 1 year, 8 months ago

I think the wording of option A has a typo first it mentioned " Update the application to retrieve the variables from AWS Systems Manager Parameter Store" then it says "Store the credentials in AWS Secrets Manager in each environment."

upvoted 1 times

🗨️ **meetparag81** 1 year, 8 months ago

A is correct

upvoted 1 times

🗨️ **jayvarma** 1 year, 9 months ago

Option A is correct. The AWS Systems Manager Paramter Store's primary purpose is to secure sensitive information such as API URLs, credentials and the variables that we store in it.

upvoted 2 times

🗨️ **MrTee** 2 years ago

**Selected Answer: A**

his solution allows the developer to securely store and retrieve different types of variables, including authentication information for a remote API, the URL for the API, and credentials.

upvoted 2 times

🗨️ **qsergii** 2 years, 1 month ago

Definitely A

upvoted 1 times

🗨️ **fqmark** 2 years, 1 month ago

it should be a, kms is used for encryption: <https://aws.amazon.com/kms/>

upvoted 3 times