

Microsoft Discussions



Exam AZ-900 All Questions

View all questions & answers for the AZ-900 exam

Go to Exam

EXAM AZ-900 TOPIC 1 QUESTION 273 DISCUSSION

Actual exam question from Microsoft's AZ-900

Question #: 273

Topic #: 1

[\[All AZ-900 Questions\]](#)

To what should an application connect to retrieve security tokens?

- A. an Azure Storage account
- B. Azure Active Directory (Azure AD)
- C. a certificate store
- D. an Azure key vault

Show Suggested Answer

by [vanr2000](#) at July 29, 2019, 9:29 p.m.

Comments

Type your comment...

Submit

[vanr2000](#) **Highly Voted** 5 years, 2 months ago

It should be D, instead of B. Azure key vault keep Security Tokens

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-what-is>

👍 ↩ 🚩 upvoted 185 times

🗨️ 👤 **Nathan12345** 2 months ago

Its B. D is wrong. Please verify.

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **JustSignalingVirtues** 2 years, 5 months ago

Security Token is not a Secret. Password, Private Keys, Certificates, etc., are secrets. Tokens are generated when request is made and they change with almost each request and valid for short duration only. So, there is no point in protecting the token by storing it in the vault to use it when needed, it is not a static value.

👍 ↩ 🚩 upvoted 11 times

🗨️ 👤 **exam_taker5** 5 years, 2 months ago

agreed

👍 ↩ 🚩 upvoted 9 times

🗨️ 👤 **Sisb** 2 years, 9 months ago

D token , API key are in key Vault.

👍 ↩ 🚩 upvoted 1 times

[Load full discussion...](#)

🗨️ 👤 **RTT1976** Highly Voted 4 years, 12 months ago

The answer B is correct, because it asks what "an application should connect to".
An Application cannot connect to a Key Vault.

👍 ↩ 🚩 upvoted 67 times

🗨️ 👤 **Christian_garcia_martin** 3 months, 2 weeks ago

humm, if your app is hosted in app service how it replace the values in appSettings if it can not connect to the key vault?

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **richardsonbq** 4 years, 11 months ago

Actually, the Key Vault can be accessed by an Application to retrieve secure information. So I'm not sure if AD is the only right answer here...

👍 ↩ 🚩 upvoted 8 times

🗨️ 👤 **vsivas** 4 years, 10 months ago

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory-b2c/active-directory-b2c-apps> AD is correct

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **richardsonbq** 4 years, 11 months ago

But in the context of the answer, I believe AD is more appropriate as per <https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-scenarios#security-tokens>

👍 ↩ 🚩 upvoted 7 times

🗨️ 👤 **clouddba** 3 years, 4 months ago

Totally agree with you richardsonbq :)

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **clouddba** 3 years, 4 months ago

Finally! :) Absolutely agree

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **126e81f** Most Recent 2 months, 1 week ago

Azure Key Vault is a service used to securely store and manage secrets, keys, and certificates, but it is not used for retrieving security tokens for application authentication or authorization. Instead, Azure Active Directory (Azure AD) is the service used for obtaining and managing security tokens.

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **Genichiro** 2 months, 2 weeks ago

The correct answer is B.

An application should connect to Azure Active Directory (Azure AD) to retrieve security tokens. Azure AD is the identity provider that issues security tokens for authentication and authorization purposes¹².

Azure Key Vault, on the other hand, is used to securely store secrets, such as API keys, passwords, and certificates, but it is not used to issue security tokens².

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **Christian_garcia_martin** 3 months, 2 weeks ago

the question is right , it says applications security tokens not users , and of course application connect to key vault to can replace values of appSettings properties

replace values of appSettings properties

👍 ↩ 🚩 upvoted 2 times

🗲️ 👤 **Nicosi** 3 months, 3 weeks ago

imho it is B, <https://learn.microsoft.com/en-us/azure/key-vault/general/authentication> - check the diagram

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **siculoct** 4 months, 3 weeks ago

Its D

Storing Application Secrets:

API Keys and Tokens: Securely store API keys, tokens, and other sensitive configuration data that applications need to access.

Database Connection Strings: Store connection strings securely and retrieve them as needed for application configuration.

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **linux_admin** 7 months ago

Selected Answer: B

When an application needs to authenticate itself or a user to access another service, it typically requests a security token from Azure AD, which validates the credentials and returns a token that the application can use to access the desired service.

👍 ↩ 🚩 upvoted 3 times

🗲️ 👤 **4pelos** 9 months, 1 week ago

Answer D

In the context of Azure and authentication, an application typically connects to Azure Active Directory (Azure AD) to retrieve security tokens. Azure AD is Microsoft's cloud-based identity and access management service that helps your users sign in and access resources

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **4pelos** 9 months, 1 week ago

Sorry B - Azure Active Directory (Azure AD)

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **az900k** 9 months, 2 weeks ago

Selected Answer: B

Azure AD authenticates users and provides access tokens. Key Vault stores it.

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **DogDaddy** 1 year ago

Key vault stores tokens, AAD is used to retrieve them

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **Ada_Ada** 1 year ago

To retrieve security tokens, applications should connect to key vault and users should connect to AAD

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **Taus** 1 year, 3 months ago

I agree with B.

When an application needs to retrieve security tokens, it should connect to Azure AD. Azure AD issues security tokens, such as OAuth2 access tokens, OpenID Connect ID tokens, and SAML tokens, to users and applications after they have been authenticated.

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **petebear55** 1 year, 4 months ago

b is the correct answer :

<https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-scenarios>

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **zimzimzimma** 1 year, 4 months ago

I'm voting for B. I am interpreting 'Receiving security tokens' as a set of claims when you connect to... Azure AD.

👍 ↩ 🚩 upvoted 2 times

🗲️ 👤 **zimzimzimma** 1 year, 4 months ago

Addendum to myself: See <https://learn.microsoft.com/en-us/azure/active-directory/develop/security-tokens>

It's definitely Azure AD.

👍 ↩ 🚩 upvoted 1 times

🗲️ 👤 **speedyweedy** 1 year, 5 months ago

Selected Answer: B

An application should connect to the Azure Active Directory (Azure AD) authentication endpoint to retrieve security tokens.



Azure AD provides different authentication endpoints for different scenarios, but the most common endpoint used to retrieve security tokens is the OAuth 2.0 authorization endpoint. The endpoint URL is typically formatted as follows:

```
```\nhttps://login.microsoftonline.com/{tenant}/oauth2/v2.0/token\n```\n
```

Where `{tenant}` is the name or ID of the Azure AD tenant that the application is registered in.

To retrieve an access token from the OAuth 2.0 authorization endpoint, the application must first obtain an authorization code from the Azure AD authorization endpoint. The authorization code is obtained by redirecting the user to a sign-in page, where the user signs in with their Azure AD credentials and consents to the application's requested permissions.

   upvoted 4 times

  **C4rlos** 1 year, 7 months ago

**Selected Answer: D**

D is the correct answer.

   upvoted 2 times

[Load full discussion...](#)

**Start Learning for free**



### Social Media

[Facebook](#) , [Twitter](#)

[YouTube](#) , [Reddit](#)

[Pinterest](#)



We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.



© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.