NOTE: Each correct selection is worth one point.

A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key

Correct Answer: CE
Explanation:
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

References:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

QUESTION 19
You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.

What should you create first?

A. an Azure Application Insights service
B. an Azure DevOps organization
C. an Azure Storage account
D. an Azure DevTest Labs lab

Correct Answer: B

QUESTION 20
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

A. Yes
B. No

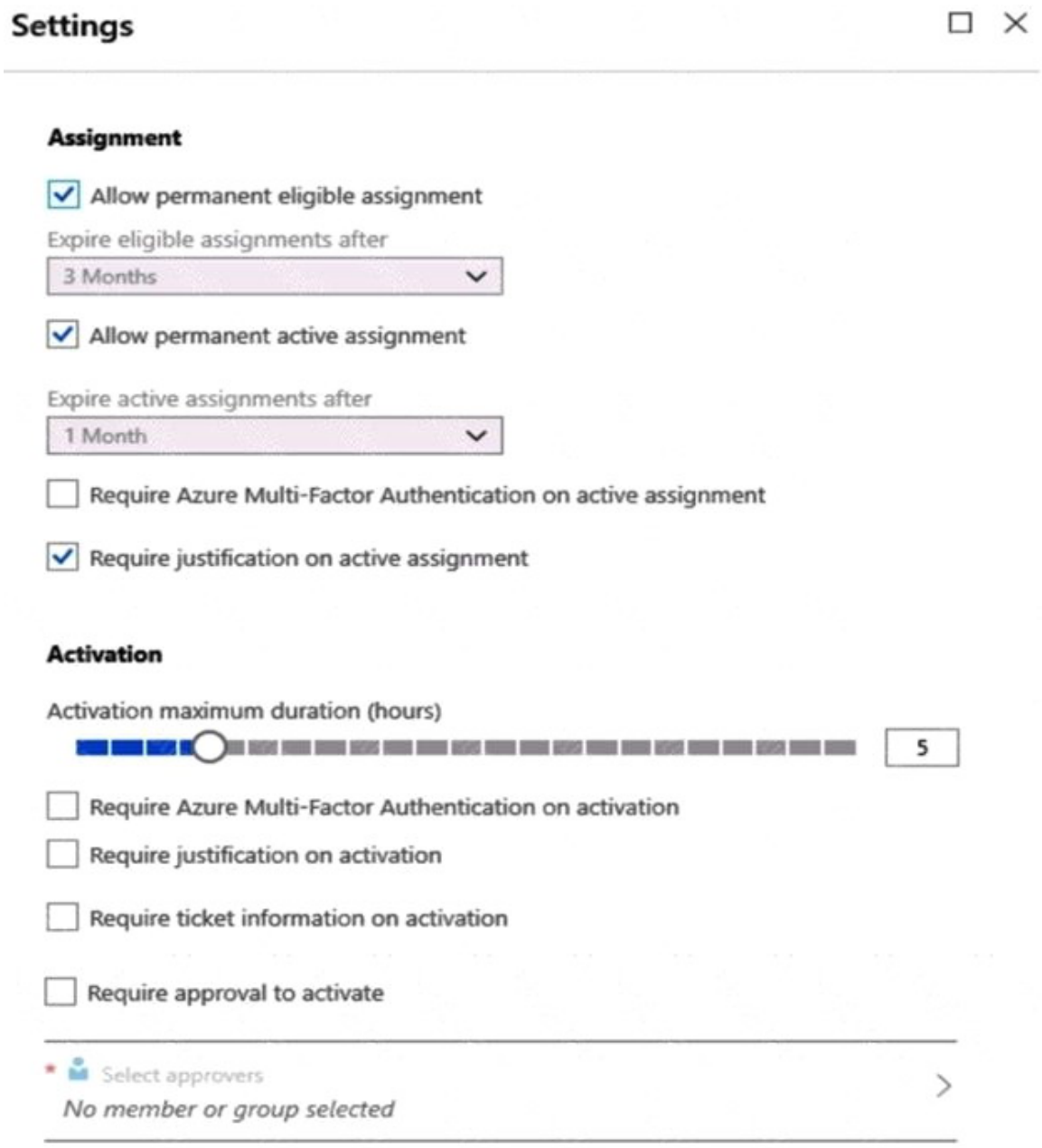
Correct Answer: B
Explanation:
Microsoft Antimalware is deployed as an extension and not a feature.

References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

QUESTION 21
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.



From PIM, you assign the Security Administrator role to the following groups:

- Group1: Active assignment type, permanently assigned
- Group2: Eligible assignment type, permanently eligible

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

Correct Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

QUESTION 22
Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

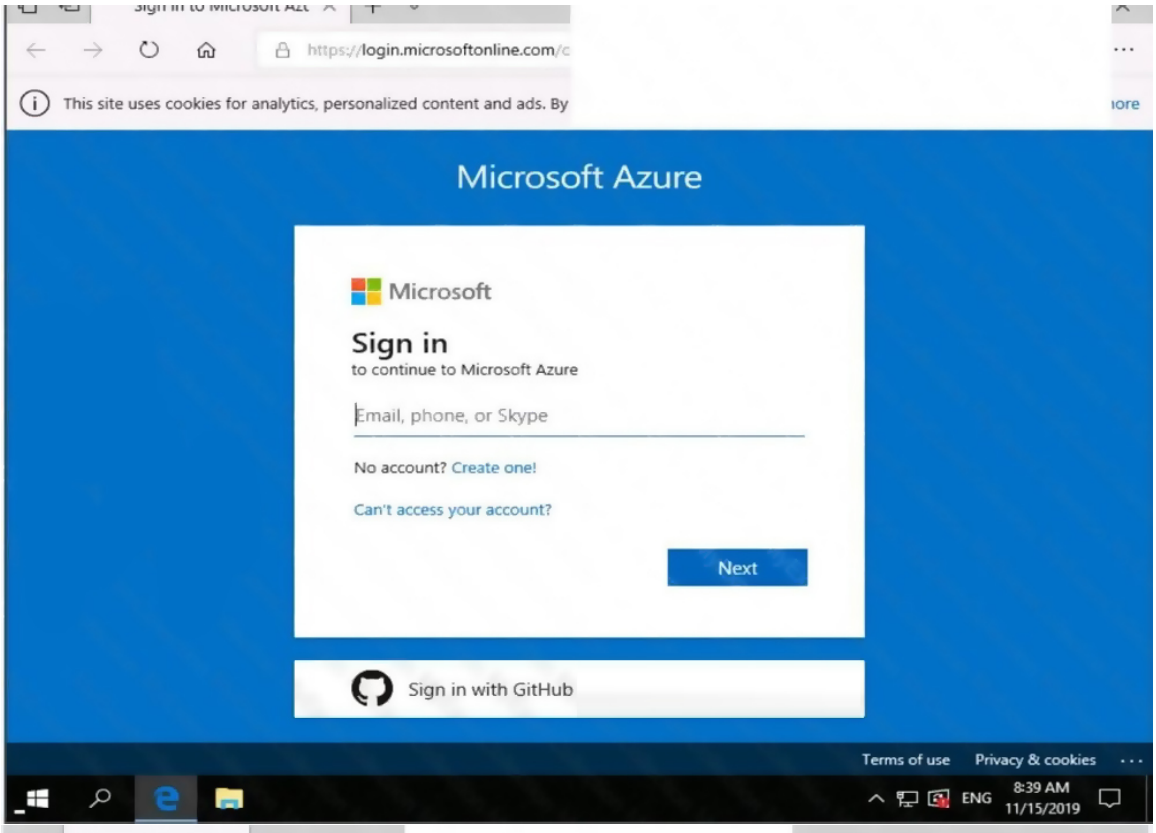
Azure Username: User1-10598168@ExamUsers.com

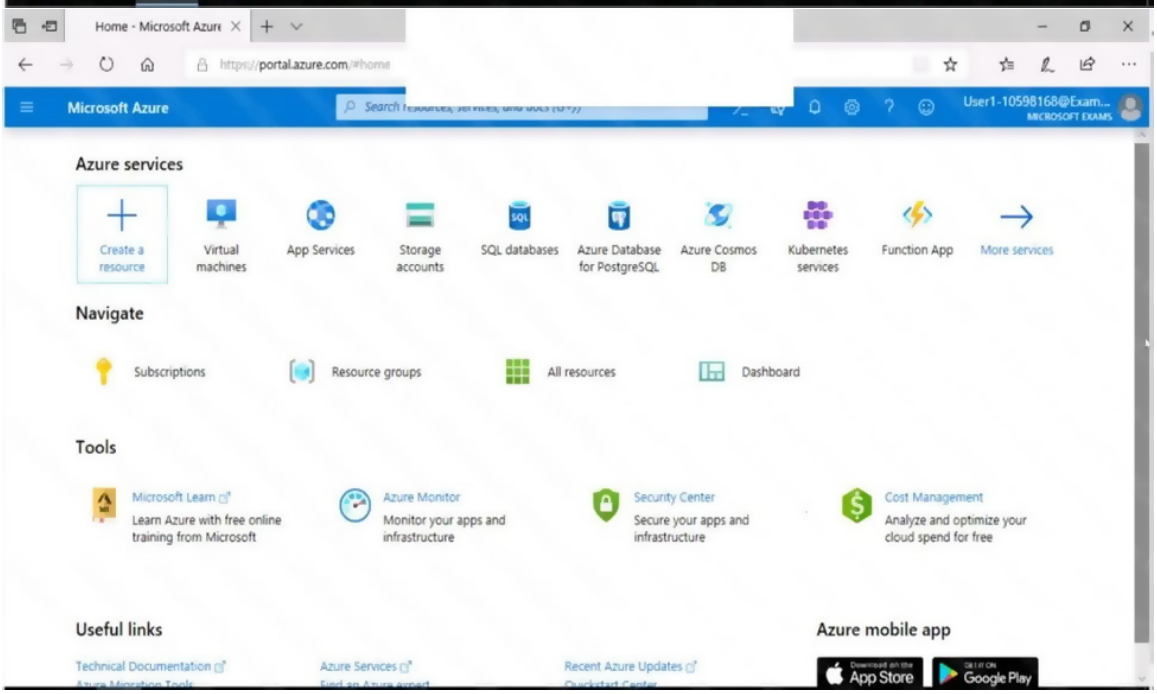
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168

[Download Full Version AZ-500 Exam Dumps(Updated in Feb/2023)]





[AZ-500 Exam Dumps] [AZ-500 PDF Dumps] [AZ-500 VCE Dumps] [AZ-500 Q&As]
https://www.ensurepass.com/AZ-500.html