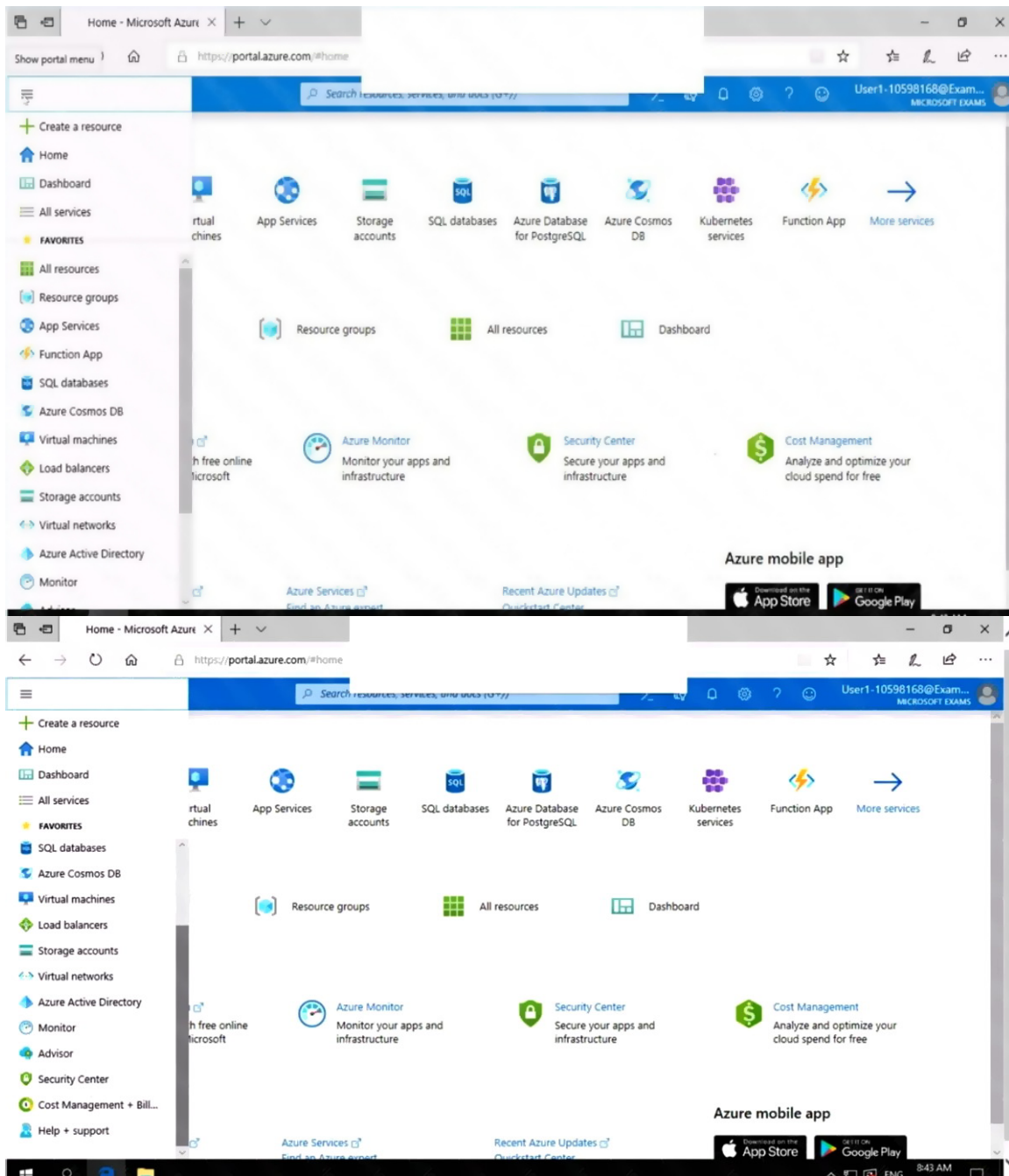


## [Download Full Version AZ-500 Exam Dumps\(Updated in Feb/2023\)](#)

The image shows a screenshot of a web browser displaying the Microsoft Azure login page. The browser's address bar shows the URL <https://login.microsoftonline.com/>. A cookie notice at the top states: "This site uses cookies for analytics, personalized content and ads. By". The main content area has a blue header with "Microsoft Azure" and a white sign-in box. The sign-in box contains the Microsoft logo, the text "Sign in to continue to Microsoft Azure", a text input field for "Email, phone, or Skype", and links for "No account? Create one!" and "Can't access your account?". A "Next" button is at the bottom right of the sign-in box. Below the sign-in box is a "Sign in with GitHub" button. The browser's taskbar at the bottom shows the Windows Start button, search icon, and several open applications. The browser's address bar also shows the URL <https://portal.azure.com/#home>. The Azure portal dashboard is visible, featuring a search bar, a "Create a resource" button, and various service tiles including Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, and Function App. The "Navigate" section includes links for Subscriptions, Resource groups, All resources, and Dashboard. The "Tools" section includes links for Microsoft Learn, Azure Monitor, Security Center, and Cost Management. The "Useful links" section includes links for Technical Documentation, Azure Services, and Recent Azure Updates. The "Azure mobile app" section includes links for the App Store and Google Play.

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

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



You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

To complete this task, sign in to the Azure portal.

**Correct Answer:** See the explanation below.

**Explanation:**

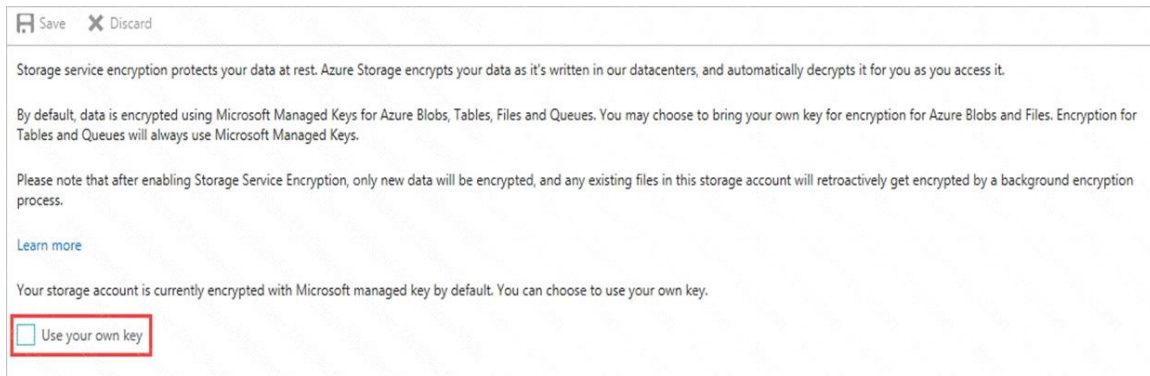
Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

[AZ-500 Exam Dumps](#)   [AZ-500 PDF Dumps](#)   [AZ-500 VCE Dumps](#)   [AZ-500 Q&As](#)

<https://www.ensurepass.com/AZ-500.html>

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

1. Navigate to your storage account rg1lod10598168n1
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.



Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

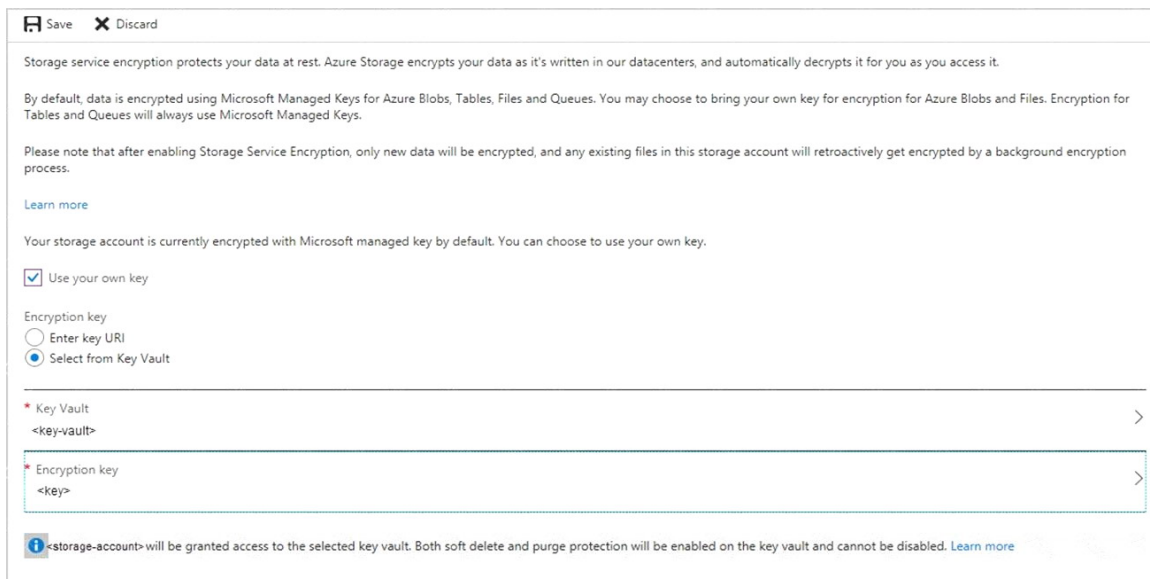
Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

### Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

4. Choose the Select from Key Vault option.
5. Choose the key vault KeyVault10598168 containing the key you want to use.
6. Choose the key from the key vault.



Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key

☐ Enter key URI

☒ Select from Key Vault

\* Key Vault  
<key-vault>

\* Encryption key  
<key>

<storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

### Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal>

[AZ-500 Exam Dumps](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#) [AZ-500 Q&As](#)

<https://www.ensurepass.com/AZ-500.html>

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

### **QUESTION 77**

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and assignments that are scoped to resource groups.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: A**

### **QUESTION 78**

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: A**

**Explanation:**

**[AZ-500 Exam Dumps](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#) [AZ-500 Q&As](#)**

**<https://www.ensurepass.com/AZ-500.html>**

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

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

### QUESTION 79

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

- Name: VM1
- Size: DS2v2
- Resource group: RG1
- Region: West Europe
- Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only
- D. Vault1 or Vault2 only

**Correct Answer: A**

#### **Explanation:**

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

### QUESTION 80

#### HOTSPOT

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

[AZ-500 Exam Dumps](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#) [AZ-500 Q&As](#)

<https://www.ensurepass.com/AZ-500.html>