



Free Questions for *AZ-500* by *go4braindumps*

Shared by *Horton* on *07-06-2022*

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

You have the hierarchy of Azure resources shown in the following exhibit.


 Image not found or type unknown

You create the Azure Blueprints definitions shown in the following table.

 Image not found or type unknown

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

 Image not found or type unknown

Blueprints can only be assigned to subscriptions.

Answer:

Question 2

Question Type: MultipleChoice

A user named Debbie has the Azure app installed on her mobile device.

You need to ensure that `debbie@contoso.com` is alerted when a resource lock is deleted.

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

You need to configure an alert rule in Azure Monitor.

Type Monitor into the search box and select Monitor from the search results.

Click on Alerts.

Click on +New Alert Rule.

In the Scope section, click on the Select resource link.

In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results.

Select the subscription then click the Done button.

In the Condition section, click on the Select condition link.

Select the Delete management locks condition then click the Done button.

In the Action group section, click on the Select action group link.

Click the Create action group button to create a new action group.

Give the group a name such as Debbie Mobile App (it doesn't matter what name you enter for the exam) then click the Next: Notifications > button.

In the Notification type box, select the Email/SMS message/Push/Voice option.

In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter debbie@contoso.com in the Azure account email field.

Click the OK button to close the window.

Options:

- A) Enter a name such as Debbie Mobile App in the notification name box.
- B) Click the Review & Create button then click the Create button to create the action group.
- C) Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.
- D) Click the Create alert rule button to create the alert rule.

Answer:

A

Question 3

Question Type: Hotspot

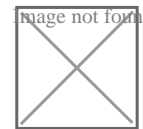
On Monday, you configure an email notification in Azure Security Center to email notifications to user1@contoso.com.

On Tuesday, Security Center generates the security alerts shown in the following table.



How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

Question 4

Question Type: MultipleChoice

You have an Azure subscription that contains the storage accounts show in the following table.

Image not found or type unknown



You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

Options:

A) Explanation:

Answer as in image

storage1: Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD) ▼

storage2: Shared Key only ▼

storage3: Shared access signature (SAS) only ▼

Answer:

A

Question 5

Question Type: Hotspot

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

with the following settings:

*Conditions: Sign-in risk level: Medium and above

*Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

When User1 signs in from an anonymous IP address, the user will:

Answer:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

Question 6
When User2 signs in from an unfamiliar location, the user will:

Question Type: MultipleChoice

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

SIMULATION

When User3 signs in from an infected device, the user will:

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


	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

sign in to microsoft AZURE

https://login.microsoftonline.com/c

This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

 Microsoft

Sign in


to continue to Microsoft Azure

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Next

 Sign in with GitHub

Terms of use Privacy & cookies

8:39 AM
11/15/2019

Home - Microsoft Azure X +

https://portal.azure.com/#home

Microsoft Azure Search Resources, services, and more (0/77)

User1-10598168@Exam... MICROSOFT EXAMS

Azure services

- Create a resource
- Virtual machines
- App Services
- Storage accounts
- SQL databases
- Azure Database for PostgreSQL
- Azure Cosmos DB
- Kubernetes services
- Function App
- More services

Navigate

- Subscriptions
- Resource groups
- All resources
- Dashboard

Tools

- Microsoft Learn [↗]
Learn Azure with free online training from Microsoft
- Azure Monitor [↗]
Monitor your apps and infrastructure
- Security Center [↗]
Secure your apps and infrastructure
- Cost Management [↗]
Analyze and optimize your cloud spend for free

Useful links

- Technical Documentation [↗]
- Azure Migration Tools [↗]
- Azure Services [↗]
Find an Azure expert
- Recent Azure Updates [↗]
- Quickstart Center [↗]

Azure mobile app

Download on the App Store | GET IT ON Google Play

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor

Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, Function App, More services

Resource groups, All resources, Dashboard

Azure Monitor: Monitor your apps and infrastructure
Security Center: Secure your apps and infrastructure
Cost Management: Analyze and optimize your cloud spend for free

Azure Services, Recent Azure Updates, Azure mobile app, App Store, Google Play

- Home
- Dashboard
- All services
- FAVORITES
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Bill...
- Help + support

Search resources, services, and docs (0/7)

Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, Function App, More services

Resource groups, All resources, Dashboard

with free online Microsoft, Azure Monitor: Monitor your apps and infrastructure, Security Center: Secure your apps and infrastructure, Cost Management: Analyze and optimize your cloud spend for free

Azure mobile app
 Download on the App Store | GET IT ON Google Play

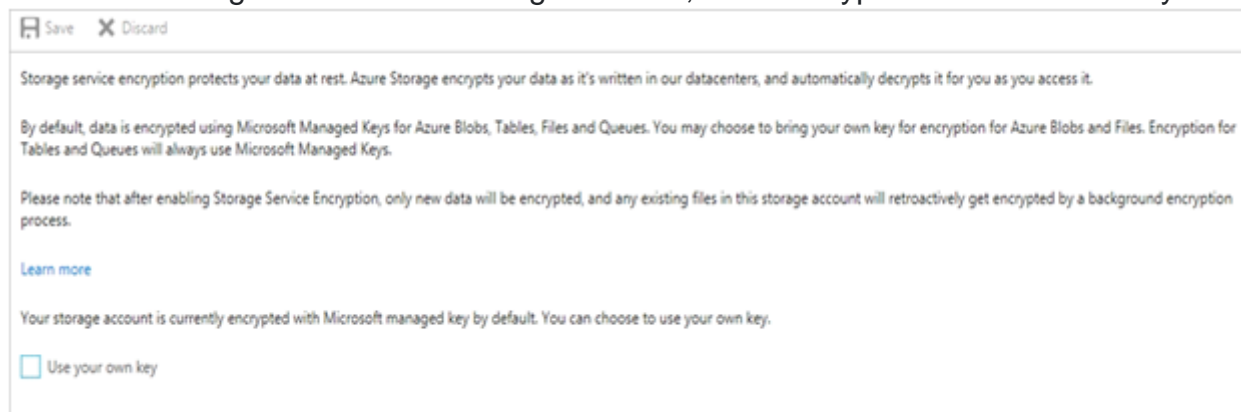
You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

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

Options:

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

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.

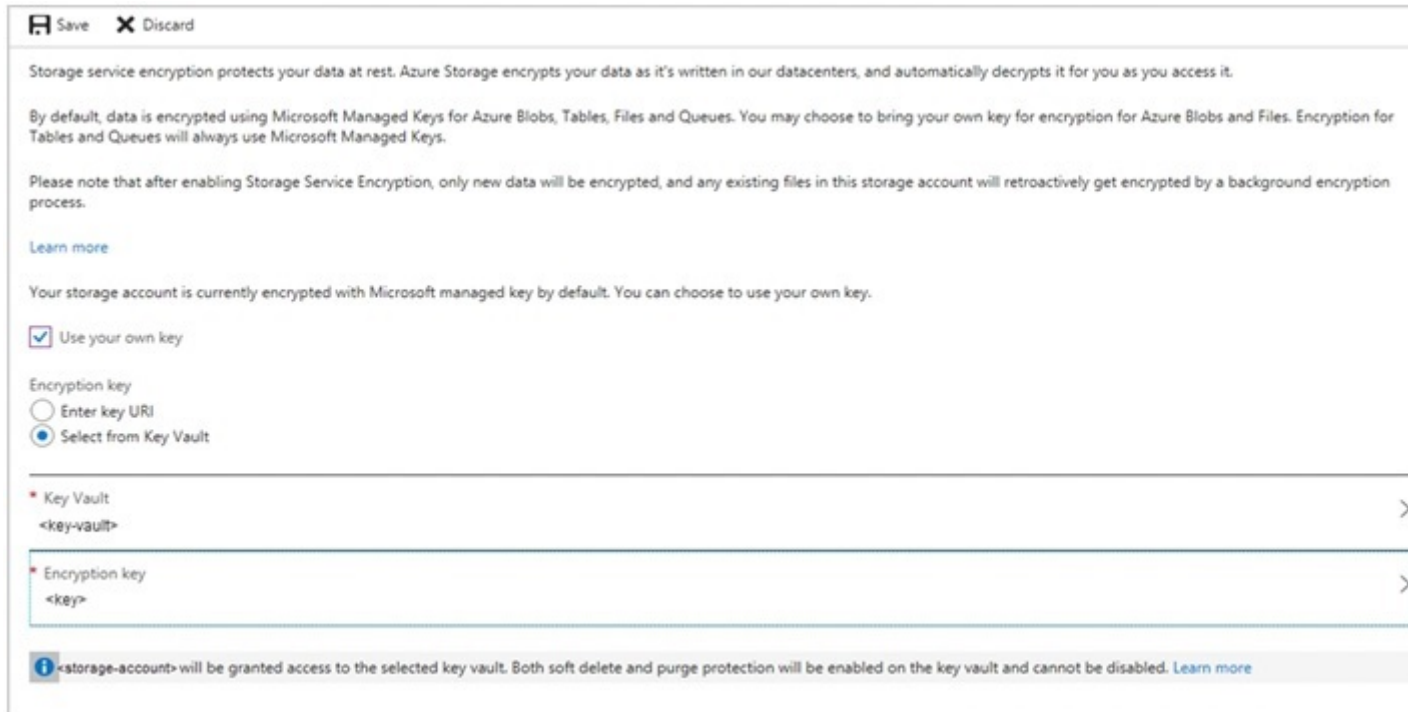


Step 2: Specify a key from a key vault

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> >

i <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](#)

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

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 X 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>

i <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](#)

Answer:

A

Explanation:

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

Question 7

Question Type: MultipleChoice

SIMULATION

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

sign in to microsoft AZURE

https://login.microsoftonline.com/c

This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

 Microsoft

Sign in


to continue to Microsoft Azure

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Next](#)

 Sign in with GitHub

Terms of use Privacy & cookies ...

8:39 AM
11/15/2019

Home - Microsoft Azure x + v

https://portal.azure.com/#home

Microsoft Azure Search resources, services, and docs (0/7)

User1-10598168@Exam... MICROSOFT EXAMS

Azure services

- Create a resource
- Virtual machines
- App Services
- Storage accounts
- SQL databases
- Azure Database for PostgreSQL
- Azure Cosmos DB
- Kubernetes services
- Function App
- More services

Navigate

- Subscriptions
- Resource groups
- All resources
- Dashboard

Tools

- Microsoft Learn [Learn Azure with free online training from Microsoft](#)
- Azure Monitor [Monitor your apps and infrastructure](#)
- Security Center [Secure your apps and infrastructure](#)
- Cost Management [Analyze and optimize your cloud spend for free](#)

Useful links

- [Technical Documentation](#)
- [Azure Migration Tools](#)
- [Azure Services](#)
- [Find an Azure expert](#)
- [Recent Azure Updates](#)
- [Quickstart Center](#)

Azure mobile app

- Download on the App Store
- GET IT ON Google Play

Home - Microsoft Azure X + v

Show portal menu | <https://portal.azure.com/#home> | Search resources, services, and docs (0+)

User1-10598168@MICROSOFT

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor

Virtual machines | App Services | Storage accounts | SQL databases | Azure Database for PostgreSQL | Azure Cosmos DB | Kubernetes services | Function App | More services

Resource groups | All resources | Dashboard

Get started with free online Microsoft | Azure Monitor: Monitor your apps and infrastructure | Security Center: Secure your apps and infrastructure | Cost Management: Analyze and optimize your cloud spend for free

Azure Services | Recent Azure Updates

Azure mobile app

Download on the App Store | GET IT ON Google Play

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Bill...
- Help + support

Virtual machines App Services Storage accounts SQL databases Azure Database for PostgreSQL Azure Cosmos DB Kubernetes services Function App More services

Resource groups All resources Dashboard

with free online Microsoft **Azure Monitor** Monitor your apps and infrastructure **Security Center** Secure your apps and infrastructure **Cost Management** Analyze and optimize your cloud spend for free

Azure mobile app

Download on the **App Store** GET IT ON **Google Play**

[Azure Services](#) Find an Azure expert [Recent Azure Updates](#) Quickstart Center

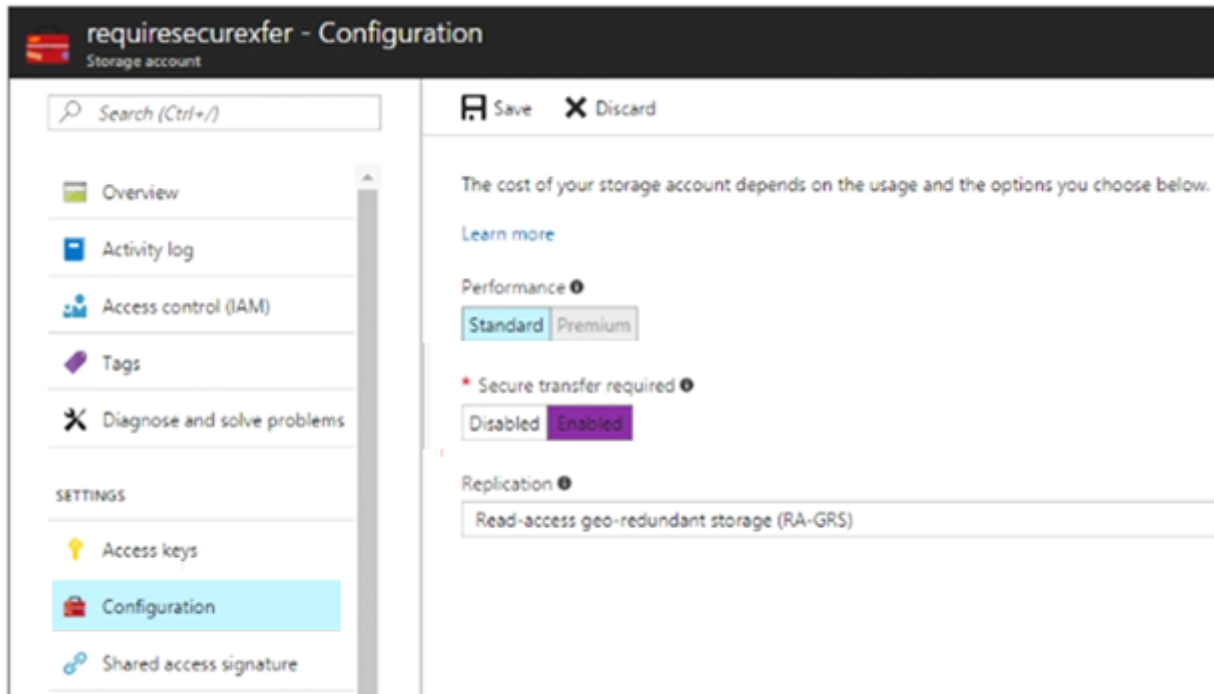
You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.

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

Options:

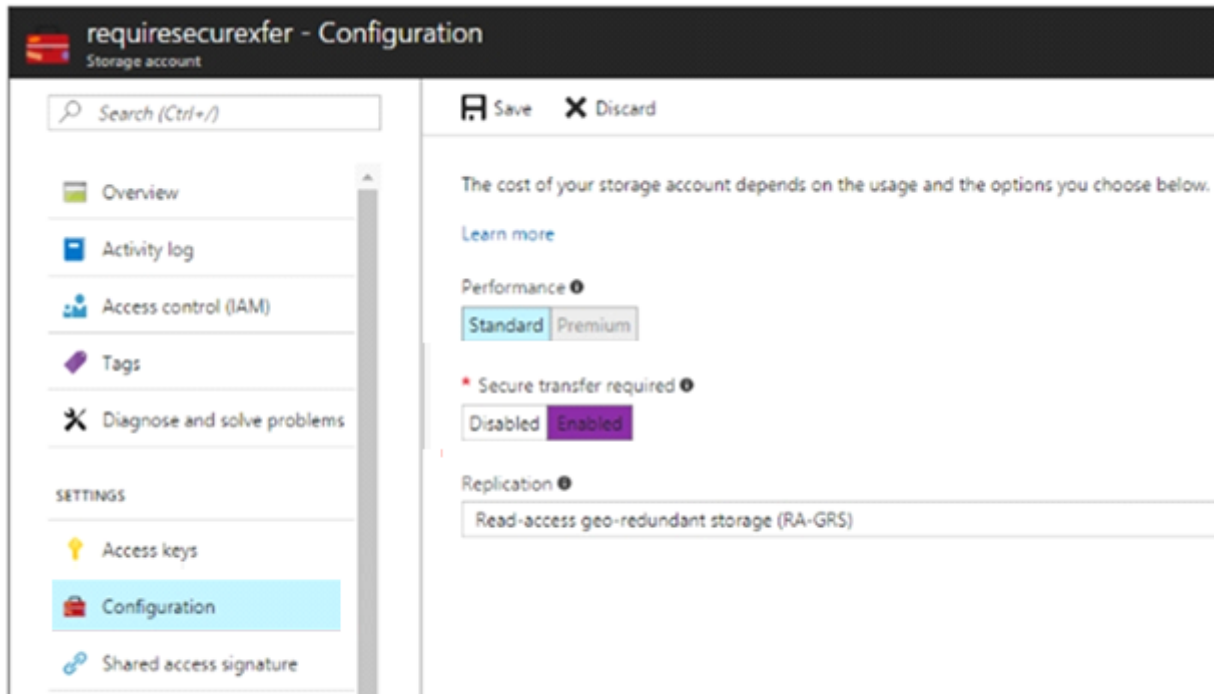
A) The 'Secure transfer required' feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
2. Select Configuration, and Secure Transfer required.



B) The 'Secure transfer required' feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
2. Select Configuration, and Secure Transfer required.



Answer:

A

Explanation:

Question 8

Question Type: MultipleChoice

SIMULATION

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

sign in to microsoft AZURE

https://login.microsoftonline.com/c

This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

 Microsoft


Sign in

to continue to Microsoft Azure

No account? [Create one!](#)

[Can't access your account?](#)

[Next](#)

 Sign in with GitHub

Terms of use Privacy & cookies ...

8:39 AM
11/15/2019

Azure services

[Create a resource](#) Virtual machines App Services Storage accounts SQL databases Azure Database for PostgreSQL Azure Cosmos DB Kubernetes services Function App [More services](#)

Navigate

[Subscriptions](#) [Resource groups](#) [All resources](#) [Dashboard](#)

Tools

[Microsoft Learn](#) Learn Azure with free online training from Microsoft [Azure Monitor](#) Monitor your apps and infrastructure [Security Center](#) Secure your apps and infrastructure [Cost Management](#) Analyze and optimize your cloud spend for free

Useful links

[Technical Documentation](#) [Azure Services](#) [Recent Azure Updates](#)

Azure mobile app

Download on the App Store GET IT ON Google Play

Home - Microsoft Azure X +

https://portal.azure.com/#home

Show portal menu

Search resources, services, and docs (0/77)

User1-10598168@Exam MICROSOFT EXAM

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Resource groups

All resources

Dashboard

with free online microsoft

Azure Monitor
Monitor your apps and infrastructure

Security Center
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

Azure Services Find an Azure expert

Recent Azure Updates Quickstart Center

Azure mobile app

Download on the App Store

GET IT ON Google Play

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Bill...
- Help + support

Search resources, services, and docs (0/77)

Virtual machines App Services Storage accounts SQL databases Azure Database for PostgreSQL Azure Cosmos DB Kubernetes services Function App More services

Resource groups All resources Dashboard

Learn more about Azure services with free online training from Microsoft

Azure Monitor
Monitor your apps and infrastructure

Security Center
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

Azure mobile app

Download on the App Store

GET IT ON Google Play

[Azure Services](#) Find an Azure expert

[Recent Azure Updates](#) Quickstart Center

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

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

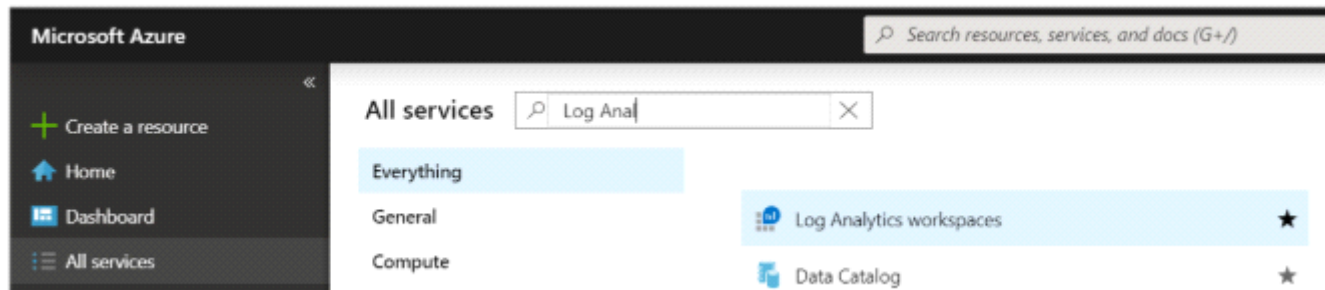
This task might take several minutes to complete. You can perform other tasks while the task completes.

Options:

A) Step 1: Create a workspace

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.



2. Select Create, and then select choices for the following items:

Log Analytics workspace

Create new or link existing workspace

Create New Link Existing

* Log Analytics Workspace ⓘ

DefaultLAWorkspace ✓

* Subscription

Microsoft Azure ▼

* Resource group

Prod ▼

[Create new](#)

* Location

East US ▼

* Pricing tier

Per GB (2018) >

3. After providing the required information on the Log Analytics workspace pane, select OK.

While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension

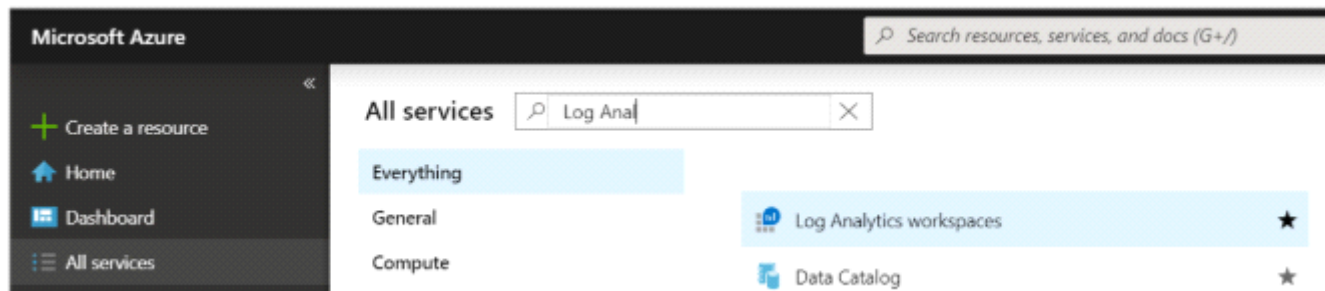
Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.
 2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).
 3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.
 4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.
 5. In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.
- After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.

B) Step 1: Create a workspace

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.



2. Select Create, and then select choices for the following items:
3. After providing the required information on the Log Analytics workspace pane, select OK.

While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension

Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.
2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).
3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.
4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.

After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.

Answer:

A

To Get Premium Files for AZ-500 Visit

<https://www.p2pexams.com/products/az-500>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/az-500>

