itrenzheng

练习题

质量更高　　服务更好

https://www.itrenzheng.com

一年免费更新服务

Exam : **AZ-104**

Title : Microsoft Azure Administrator

Version: DEMO

1. Topic 1, A. Datum Corporation

Overview

A. Datum Corporation is a consulting firm that has a main office in Montreal and branch offices in Seattle and New York.

Azure Environment

A. Datum has an Azure subscription that contains three resource groups named RG1. RG2, and RG3.
The subscription contains the storage accounts shown in the following table.

Name	Kind	Location	Hierarchical namespace	Container	File share
storage1	StorageV2	West US	Yes	cont1	share1
storage2	StorageV2	West US	No	cont2	share2

The subscription .contains the virtual machines shown in the following table.

Name	Size	Operating system	Description
VM1	A	Red Hat Enterprise Linux (RHEL)	Uses ephemeral OS disks
VM2	D	Windows Server 2022	Has a basic volume
VM3	B	Red Hat Enterprise Linux (RHEL)	Uses a standard SSDs
VM4	M	Windows Server 2022	Uses Write Accelerator disks
VM5	E	Windows Server 2022	Has a dynamic volume

The subscription has an Azure container registry that contains the images shown in the following table.

Name	Operating system
Image1	Windows Server
Image2	Linux

The subscription contains the resources shown in the following table.

Name	Description	In resource group
Workspace	Log Analytics workspace	RG1
WebApp1	Azure App Service web app	RG1
VNet1	Virtual network	RG2
zone1.com	Azure Private DNS zone	RG3

The subscription contains an Azure key vault named VaultI.
Vault! contains the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCS #12	RSA	2048
Cert2	PKCS #12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

Vaultl contains the keys shown in the following table.

Name	Type	Description
Key1	RSA	Has a key size of 4096
Key2	EC	Has Elliptic curve name set to P-256

Microsoft Entra Environment

A. Datum has a Microsoft Entra tenant named adatum.com that is linked to the Azure subscription and contains the users shown in the following table.

The lenant contains the groups shown in the following table.

Name	Type
Group1	Security group
Group2	Microsoft 365 group

The adatum.com tenant has a custom security attribute named Attribute1.

Planned Changes

A. Datum plans to implement the following changes:

• Configure a data collection rule {DCR) named DCR1 to collect only system events that have an event ID of 4648 from VM2 and VM4.

• In storage1, create a new container named cont2 that has the following access policies:

o Three stored access policies named Stored 1, Stored2, and Stored3

o A legal hold for immutable blob storage

• Whenever possible, use directories to organize storage account content.

• Grant User1 the permissions required to link Zone1 to VNet1.

• Assign Attribute1 to supported adatum.com resources.

• In storage2, create an encryption scope named Scope"1.

• Deploy new containers by using Image1 or Image2.

Technical Requirements

A. Datum must meet the following technical requirements:

• UseTLSforWebApp1.

• Follow the principle of least privilege.

• Grant permissions at the required scope only.

• Ensure that Scope1 is used to encrypt storage services.

• Use Azure Backup to back up cont1 and share1 as frequently as possible.
• Whenever possible, use Azure Disk Encryption and a key encryption key (KEK) to encrypt the virtual machines.

You need to implement the planned changes for the storage account content.
For the existing containers and file shares listed in the storage-account table, which support native directories rather than blob-name prefixes?
A. share1 only
B. cont1 and share1 only
C. share1 and share2 only
D. cont1, share1, and share2 only
E. cont1, cont2, share1, and share2
Answer: D
Explanation:
The question refers only to the existing resources in the table. storage1/cont1 supports native directories because hierarchical namespace is enabled. Both share1 and share2 are Azure Files shares and support directories independently of the Blob namespace setting. storage2/cont2 has a flat Blob namespace. Therefore D is correct. The newly planned container named cont2 in storage1 is a different resource and is outside this question's stated scope.
References:
https://learn.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-namespace
https://learn.microsoft.com/en-us/azure/storage/files/storage-files-introduction

2. You need to configure encryption for the virtual machines. The solution must meet the technical requirements.
Which virtual machines can you encrypt?
A. VM1 and VM3
B. VM2 and VM3
C. VM2 and VM4
D. VM4 and VM5
Answer: B
Explanation:
Detailed Explanation
The requirement is to use Azure Disk Encryption (ADE) with a customer key encryption key (KEK). ADE has several documented incompatibilities that eliminate three of the five VMs: it is not supported on VMs that use an ephemeral OS disk (eliminates VM1), it is not supported on disks with Write Accelerator enabled – a feature typically used on M-series VMs (eliminates VM4), and on Windows it is not supported on dynamic volumes, only basic volumes (eliminates VM5, which "has a dynamic volume"). That leaves VM2 (Windows Server 2022, basic volume) and VM3 (RHEL, an Azure-endorsed Linux distribution, standard SSD) as the only VMs ADE can encrypt with a KEK. Note also that Microsoft has announced ADE's retirement for 15 September 2028, with encryption-at-host or confidential VM OS-disk encryption recommended for new deployments.
Official Reference
Azure Disk Encryption scenarios on Windows/Linux VMs — https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows

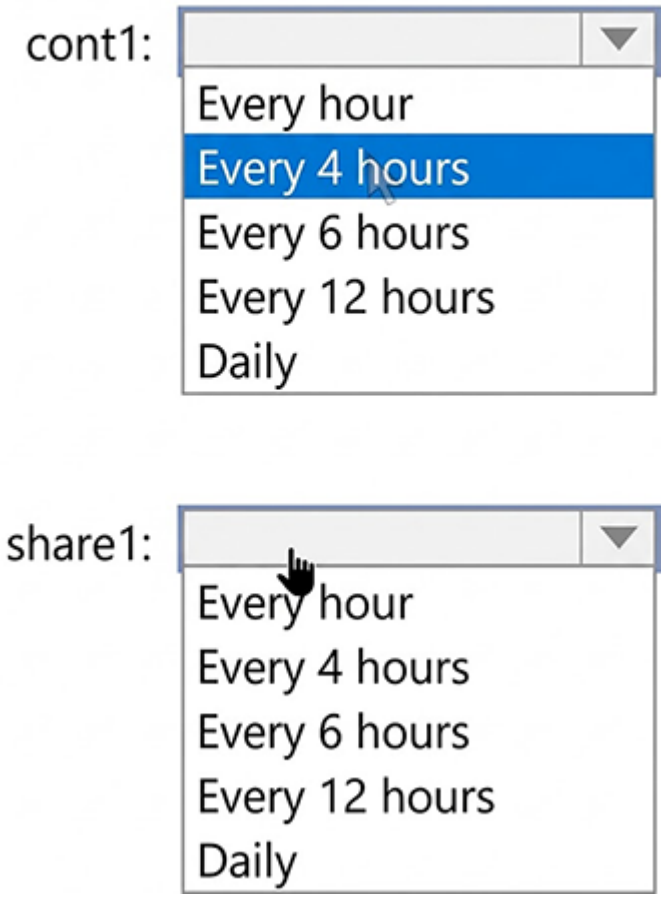
3.You implement the planned changes for Scope1.
You need to ensure that Scope1 meets the technical requirements.
What can you encrypt by using Scope1?
A. containers and blobs in storage2 only
B. containers and blobs in storage1 and storage2
C. containers, blobs, and file shares in storage2 only
D. containers, blobs, and file shares in storage1 and storage2
E. containers, blobs, file shares, queues, and tables in storage2 only
Answer: A
Explanation:
Detailed Explanation
Azure Storage encryption scopes are a Blob-service feature only: Microsoft Learn's "Encryption scopes for Blob storage" states a scope lets you manage encryption with a key scoped to a container or an individual blob. Scopes cannot be applied to Azure Files, Queue storage, or Table storage, and a scope is also a property of the single storage account in which it is created – Scope1 was created in storage2, so it can never protect storage1 resources. This rules out every option that mentions file shares, queues, tables, or storage1.
Option A is therefore the only technically valid choice: Scope1 can encrypt containers and blobs in storage2 only. (E) is outdated/incorrect – it describes account-level default (Microsoft-managed or customer-managed key) encryption, which does cover all data services, not a named encryption scope. Administrators should distinguish "storage account encryption" (covers Blobs, Files, Queues, Tables) from "encryption scope" (Blob-only, granular per-container/blob). To restrict Scope1's applicability further, set it as the container's default scope and optionally prevent overriding it at upload time.
Official Reference
Encryption scopes for Blob storage — https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview

4.HOTSPOT
You need to implement the planned changes for User1.
Which roles should you assign to User1, and for which resources? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Roles: [blank]. Choices: Contributor only; Network Contributor only; Private DNS Zone Contributor only; Network Contributor and Private DNS Zone Contributor only.
Resources: [blank]. Choices: RG2 only; RG3 only; VNet1 only; zone1.com only; RG2 and RG3 only; VNet1 and zone1.com only.
Answer: Private DNS Zone Contributor only; scope the assignments to VNet1 and zone1.com only.
Explanation:
Creating the link requires the private-zone virtualNetworkLinks/write action and permission to join the target VNet. The current Private DNS Zone Contributor role includes Microsoft.Network/privateDnsZones/*, Microsoft.Network/virtualNetworks/read and Microsoft.Network/virtualNetworks/join/action. Assign this role at zone1.com and at VNet1. The role on the zone does not inherit to the separately scoped VNet. Broader Contributor or Network Contributor grants are unnecessary for this task.
References:

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/networking
https://learn.microsoft.com/en-us/azure/dns/dns-faq-private
https://learn.microsoft.com/en-us/troubleshoot/azure/private-link/troubleshoot-private-endpoint-permission-denied#resolution-c

5.HOTSPOT
You need to configure Azure Backup to meet the technical requirements for cont1 and share1.
To what should you set the backup frequency for each resource? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer: HOLD — not verified. Do not use this item as a confirmed-answer practice question.
Explanation: The supplied source has missing, contradictory, or insufficient information for a verified answer. The original question number and prompt are retained for traceability. See question 5 in the accompanying correction report for the exact defect and the material required to resolve it.