Microsoft
AZ-104
Microsoft Azure Administrator Exam

Latest Version: 51.5

Question: 1

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

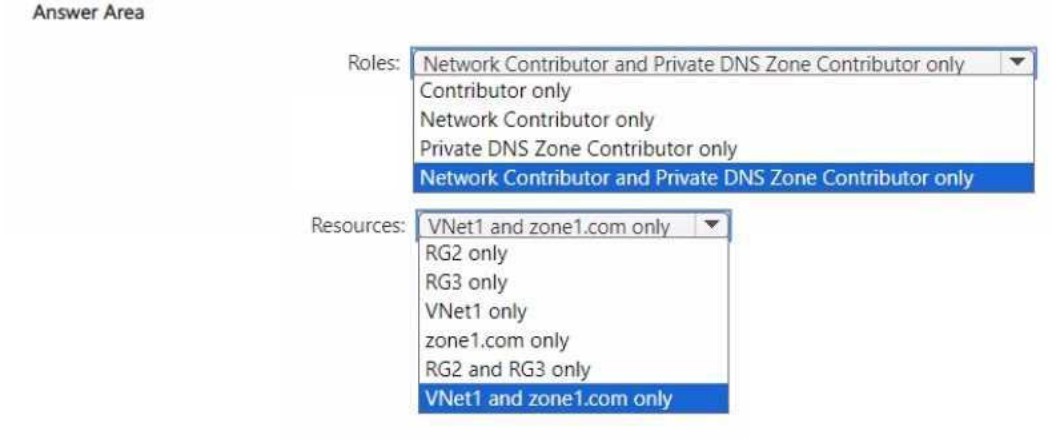
Answer: E

Explanation:
In Microsoft Azure, encryption scopes are a StorageV2 (general-purpose v2) storage account feature that allows fine-grained control over encryption settings for data stored within a single account.
According to Microsoft Azure Storage documentation, an encryption scope defines a specific encryption context that can be applied at the container or blob level and is supported in nonhierarchical namespace storage accounts (those without Data Lake Gen2 enabled).
In the given scenario:
storage1 has Hierarchical namespace = Yes (Data Lake Storage Gen2 enabled).
storage2 has Hierarchical namespace = No.
The plan was to create an encryption scope named Scope1 in storage2.
The technical requirement specifies that Scope1 must be used to encrypt storage services.
According to the Azure Administrator documentation on encryption scopes:
“Encryption scopes are supported for block blobs, append blobs, page blobs, Azure Files, queues, and tables in standard StorageV2 accounts. Encryption scopes are not supported in hierarchical namespace (Data Lake Gen2) enabled accounts.”
This means that Scope1—created in storage2, which does not have hierarchical namespace—can encrypt all blob data (containers and blobs) as well as file shares, queues, and tables.
However, storage1 cannot use encryption scopes because hierarchical namespace storage accounts (ADLS Gen2) manage encryption at the account level and do not support per-scope encryption.
Therefore, only storage2 can apply Scope1, and it can encrypt containers, blobs, file shares, queues, and tables.

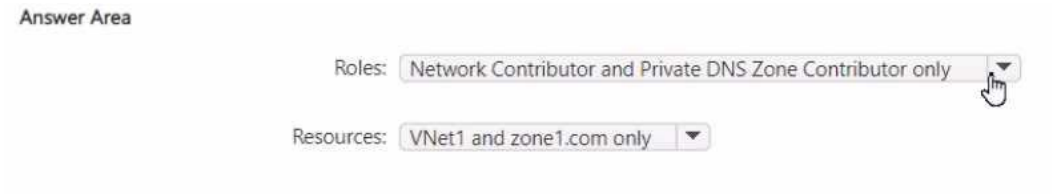
Question: 2

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.



Answer:



Explanation:
According to the Microsoft Azure Administrator (AZ-104) Study Guide and Azure Role-Based Access Control (RBAC) documentation, permissions to link an Azure Private DNS zone to a virtual network require access to both the virtual network resource and the DNS zone resource.
The process of linking a DNS zone to a virtual network establishes name resolution for the resources within that VNet through the Private DNS zone. To perform this operation, the user must have:
“Microsoft.Network/virtualNetworks/*” permissions (to modify and manage VNet settings).
“Microsoft.Network/privateDnsZones/*” permissions (to manage DNS zone links).
These permissions are granted by two built-in roles:
Network Contributor – Allows full management of the network resources like virtual networks, subnets, and network interfaces but does not allow access to manage DNS zones.
Private DNS Zone Contributor – Allows management of private DNS zones and their link configurations.
Therefore, to grant User1 the ability to link Zone1.com (Private DNS Zone) to VNet1, the correct approach is to assign both roles with the least privilege principle, scoped specifically to the required resources:
Network Contributor on VNet1
Private DNS Zone Contributor on zone1.com
Assigning the permissions at the resource level (and not at the resource group or subscription level) ensures compliance with the principle of least privilege, a core requirement of Azure governance.
This setup enables User1 to perform the exact operation (linking the Private DNS Zone to the VNet) while preventing unnecessary access to unrelated resources.
Final Verified Answe r:

 Roles: Network Contributor and Private DNS Zone Contributor only
 Resources: VNet1 and zone1.com only

Question: 3

You need to implement the planned changes for the storage account content. Which containers and file shares can you use to organize the content?

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: B

Explanation:
In the scenario, storage1 is configured as StorageV2 with Hierarchical namespace = Yes, while storage2 is configured as StorageV2 with Hierarchical namespace = No.
From Microsoft's Azure Storage Documentation and AZ-104 Study Guide, the following principles apply:
A hierarchical namespace (enabled when the storage account has Azure Data Lake Storage Gen2 capabilities) allows the use of directories within containers to organize data.
The hierarchical namespace provides directory and file-level structure similar to a file system. This is supported only for blob containers, not for Azure Files.
Azure Files (file shares) do not depend on hierarchical namespaces and cannot have directories in the same way Data Lake Gen2 does — directories can exist inside the share but not in the blob container sense.
The planned change states that you must use directories whenever possible to organize content.
Therefore, only storage accounts with hierarchical namespace enabled can use directory structures — that's storage1.
In this case:
storage1 (Hierarchical namespace = Yes) → supports containers (like cont1) and file shares (like share1).
storage2 (Hierarchical namespace = No) → does not support directories within blob containers (Data Lake structure).
Hence, you can use only cont1 (container in storage1) and share1 (file share in storage1) to organize content as required.
This is directly supported by the Microsoft documentation on Data Lake Storage Gen2:
"When you enable the hierarchical namespace for a storage account, you can organize objects into directories and subdirectories. This capability is available only for accounts configured for Data Lake Storage Gen2."
Final Verified Answe r: B. cont1 and share1 only

Question: 4

You need to implement the planned changes for DCR1. Which type of query should you use?

A. WQL
B. T-SQL
C. XPath
D. KQL

Answer: D

Explanation:
The planned change specifies that you must configure a Data Collection Rule (DCR) to collect only system events with Event ID 4648 from VM2 and VM4.
A Data Collection Rule (DCR) in Azure Monitor defines how data is collected from resources, filtered, and sent to destinations like Log Analytics workspaces. To define or query this data within Azure Monitor Logs or Log Analytics, you use Kusto Query Language (KQL).
From the Microsoft Learn: Azure Monitor Logs Documentation:
"Log queries in Azure Monitor are written in Kusto Query Language (KQL), the same query language used by Azure Data Explorer."
"KQL is optimized for querying large datasets, filtering by event IDs, sources, and event types."
Other options:
WQL (WMI Query Language) – used for on-prem Windows event querying, not for Azure DCR.
T-SQL (Transact-SQL) – used for Azure SQL Database queries, not for monitoring data.
XPath – used in Event Viewer or XML-based event filtering, not within Azure Monitor DCR configuration.
Therefore, when you configure DCR1 to collect system events (Event ID 4648) from the specified VMs, the Kusto Query Language (KQL) is the correct and verified method to filter and process these events.
Example of a valid KQL expression for this requirement:

```
SecurityEvent
| where EventID == 4648
| where Computer in ("VM2", "VM4")
```

This aligns with the Azure Monitor and Log Analytics query methodology covered in AZ-104 official exam guide (Implement and manage monitoring).

Question: 5

HOTSPOT
You need to implement the planned changes for the new containers.
Which Azure services can you use for each image? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
In Microsoft Azure, containerized application deployment can occur using multiple services, depending on the image type and operating system platform used. The question refers to two images — Image1 (Windows Server) and Image2 (Linux) — which are stored in an Azure Container Registry (ACR).
According to the Microsoft Azure Administrator Study Guide (AZ-104) and official Azure documentation, both Windows-based and Linux-based container images can be deployed using any of the following services, depending on the workload requirements:
Azure App Service (Web App for Containers) – supports both Windows and Linux containers for web applications. It allows developers to directly deploy containerized applications from Docker Hub, Azure Container Registry, or a private registry.
Azure Container Apps – serverless container hosting designed for microservices and event-driven architectures. It supports Linux and Windows containers, using Kubernetes behind the scenes, without requiring users to manage the cluster infrastructure.
Azure Container Instances (ACI) – provides lightweight, serverless containers for quick deployment and isolated workloads. It supports both Windows and Linux images and can pull directly from Azure Container Registry.
Therefore, since both Image1 (Windows Server) and Image2 (Linux) are valid container images supported by the same three Azure container services, the correct and verified solution is to select "App Service, Azure Container Apps, or Azure Container Instances" for both.
This matches Azure documentation under:
"Run containerized applications in Azure App Service"
"Deploy containers using Azure Container Instances"
"Build and deploy microservices using Azure Container Apps"

Each of these Azure services supports containerized deployments from ACR regardless of the underlying operating system image type.
Final Verified Answe r:
 Image1: App Service, Azure Container Apps, or Azure Container Instances
 Image2: App Service, Azure Container Apps, or Azure Container Instances

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer