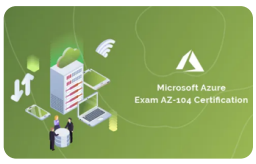


Level: Advanced

Microsoft Azure Exam AZ-104 Certification

Back to the **Course**

Implement and manage storage - **Practice Mode**

Completed on Sun, 28 Sep 2025

1st	5/15	33.33%	FAIL
Attempt	Marks Obtained	Your Score	Result

Share this Report in Social Media Share

Download Report

Domain wise Quiz Performance Report

No.	Domain	Total Question	Correct	Incorrect	Unattempted	Marked for Review
1	Implement and manage storage	15	5	10	0	0
Total	All Domains	15	5	10	0	0

Review the Answers

Filter By

Question 1

Incorrect

Domain: Implement and manage storage

A multinational corporation is planning to migrate its file storage infrastructure to Azure Cloud to enhance scalability and availability. The corporation has a diverse set of users across different geographical locations who need access to the Azure file shares.

The IT department aims to implement identity-based access control for Azure Files over SMB to ensure seamless authentication and authorization.

Which authentication options should the corporation consider? (Select 2 options)

- [ ] A. Azure role-based access control wrong

B. Azure Multi-Factor Authentication

C. On-premises AD DS authentication right

D. Azure Multi-Protocol Authentication wrong

E. Microsoft Entra Kerberos for hybrid identities right

Explanation:

Correct Answer: C and E

Option C is CORRECT because it enables users to authenticate to Azure file shares using their on-premises Active Directory credentials. It ensures seamless integration with existing identity infrastructure and enables identity-based access control for Azure Files over SMB. It enables organizations to maintain uniform access control rules, simplifying identity management and ensuring consistent access control policies across on-premises and cloud environments.

Option E is CORRECT because Microsoft Entra Kerberos for hybrid identities enables Microsoft Entra users to authenticate to Azure file shares using Kerberos authentication. It ensures proper identity-based access control for Azure Files over SMB, particularly in hybrid identity scenarios where users have both on-premises and cloud-based identities. Additionally, it enables users to access Azure file shares without requiring direct network connectivity to on-premises domain controllers, enhancing flexibility and scalability for hybrid cloud environments.

Option A is INCORRECT because Azure RBAC enables fine-grained access management for Azure resources. While it's not directly related to identity-based access control for Azure Files over SMB, it can still be used to manage access permissions for Azure resources at a broader level. However, it does not handle authentication specifically for file shares.

Option B is INCORRECT because although Azure MFA improves security by demanding multiple forms of verification during user sign-ins, it is not specifically related to authentication for Azure Files over SMB. While it provides an additional degree of protection, it doesn't handle authentication for file shares.

Option D is INCORRECT because Azure Multi-Protocol Authentication is not a recognized authentication method for Azure Files over SMB. This option is not relevant for providing identity-based access control to Azure file shares.

Reference:

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#supported-authentication-scenarios

Ask our Experts

Did you like this **Question?**

Question 2 Incorrect

Domain: Implement and manage storage

A healthcare organization is transitioning its file storage infrastructure to Azure Cloud to improve data accessibility and security. What authentication method should be prioritized for integrating with on-premises Active Directory Domain Services (AD DS) when

configuring identity-based access for Azure Files?

Proposed Solution: The healthcare organization should prioritize setting up AD domain controllers and domain-joining machines or VMs for integrating with on-premises AD DS. Is this proposed solution correct? (Select True or False)

A. True right

B. False wrong

Explanation:

Correct Answer: A

Option A is CORRECT because implementing AD domain controllers and domain-joining machines or VMs to integrate with on-premises AD DS is the recommended authentication method for configuring identity-based access to Azure files. By leveraging the organization's established AD infrastructure, the healthcare organization can maintain a cohesive identity management system, simplifying user authentication and access control processes. Prioritizing this authentication method facilitates a smooth transition to Azure Cloud storage while upholding stringent security standards and regulatory requirements.

Option B is INCORRECT because the above-proposed solution is True.

Reference:

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#how-it-works

Ask our Experts

Did you like this **Question?**

Question 3 Incorrect

Domain: Implement and manage storage

You have an Azure storage account named teststorage1. You need to enable soft delete for all the file shares in teststorage1. What is the maximum retention period you can specify?

A. 30 days

B. 90 days wrong

C. 365 days right

D. 48 hours

E. 7 days

Explanation:

Correct Answer: C

Option C is CORRECT because Azure storage accounts enable you to set a maximum retention duration of 365 days for soft delete. Allowing enough time for file shares or data to be recovered after deletion. By using soft delete you can retrieve data that has been accidentally erased or overwritten. When soft delete is enabled, data that has been erased is retained for a specified period, during which it can be recovered.

To enable soft delete for all the file shares in teststorage1 and set the file share retention period, you need to perform the following steps -

Sign in to the Azure Portal

Navigate to the storage account teststorage1

Select File shares under the Data storage column on the left pane

Select Disabled next to the Soft delete under File share settings

Select Enabled for soft delete for all file shares when the Soft delete settings panel appears

Use the slider to adjust the File share retention period in days, to specify a number between 1 to 365 days

To confirm your data retention setting click on the save button

Option A is INCORRECT because the maximum retention period for soft delete in an Azure storage account is longer than 30 days. Therefore this is not a correct option.

Option B is INCORRECT because the maximum retention period for soft delete in an Azure storage account is longer than 90 days. Therefore this is not the correct option.

Option D is INCORRECT because the maximum retention period for soft delete in an Azure storage account is much longer than 48 hours. Therefore this is not a correct option.

Option E is INCORRECT because the maximum retention period for soft delete in an Azure storage account is longer than 7 days. Therefore this is not a correct option.

Reference:

https://learn.microsoft.com/en-us/azure/storage/files/storage-files-enable-soft-delete?tabs=azure-portal#getting-started

Ask our Experts

Did you like this **Question?**

Question 4

Incorrect

Domain: Implement and manage storage

You have an Azure file share named testshare3. What should you do before deleting testshare3?

A. Rename the snapshots

B. Migrate the snapshots to another storage account

C. Disable share snapshots for testshare3

D. Delete all snapshots associated with testshare3 right

E. Convert the snapshots to read-write mode wrong

Explanation:

Correct Answer: D

Option D is CORRECT because Azure requires that all snapshots associated with a file share, in this case testshare3, be deleted before the file share itself can be deleted. This ensures that no data from the snapshots is retained inadvertently. Azure enforces a policy where a file share that contains snapshots cannot be deleted unless all the snapshots are removed first. Snapshots are point-in-time, read-only copies of data within the file share. They serve to protect and restore data in case of accidental deletions or data corruption. As long as the snapshots exist, they provide recovery points that are critical for data protection. Deleting all snapshots associated with testshare3 ensures that all potential recovery points are consciously discarded before the primary data container is removed.

Option A is INCORRECT because renaming snapshots does not allow the deletion of the file share. Snapshots need to be deleted, not renamed, to delete the file share.

Option B is INCORRECT because migrating snapshots to another storage account is not a requirement for deleting the file share. Moreover, Azure does not support directly migrating Azure files share snapshots to another storage account; snapshots must be handled within the same account.

Option C is INCORRECT because simply disabling the snapshot feature does not remove existing snapshots. The existing snapshots must be explicitly deleted before the file share can be deleted.

Option E is INCORRECT because snapshots are inherently read-only and cannot be converted to read-write mode. The snapshots must be deleted to proceed with the deletion of the file share.

Reference:

https://learn.microsoft.com/en-us/azure/storage/files/storage-snapshots-files#capabilities

Ask our Experts

Did you like this **Question?**

Question 5 Incorrect

Domain: Implement and manage storage

You have two storage accounts, testsource1, and testdestination1.

You want to replicate only specific blobs that start with “logs” from testsource1 to testdestination1. How can you achieve this during the configuration of the object replication policy?

A. Use a wildcard character in the prefix

B. Create a filter with the prefix “logs” right

C. Enable immutable storage wrong

D. Set up a lifecycle management rule

E. Use multi-protocol access

Explanation:

Correct Answer: B

Option B is CORRECT because to replicate only specific blobs that start with the prefix “logs” from testsource1 to testdestination1, you need to create a filter with the prefix “logs” in the object replication policy. This filter ensures that only blobs matching the specified prefix are replicated. Creating a filter with the prefix “logs” is the appropriate approach to replicate only specific blobs from the source storage account (testsource1) to the destination storage account (testdestination1). This filter effectively narrows down the scope of replication to include only the desired subset of blobs that meet the specified criteria.

Option A is INCORRECT because Object replication policies do not support the use of wildcard characters in prefixes. Prefix filters must specify an exact prefix to replicate specific blobs.

Option C is INCORRECT because enabling immutable storage is not directly related to configuring object replication policies. Immutable storage provides an additional layer of data protection by preventing data from being modified or deleted for a specified retention period.

Option D is INCORRECT because lifecycle management rules are used to automatically manage the lifecycle of blobs based on specified criteria such as age or access tier. They are not directly related to configuring object replication policies for replicating specific blobs with a particular prefix.

Option E is INCORRECT because multi-protocol access allows access to Azure Blob Storage using both Azure Blob Storage APIs and Azure Data Lake Storage Gen2 APIs. It does not specifically address the replication of specific blobs with a particular prefix from one storage account to another.

Reference:

https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-configure?tabs=portal#configure-object-replication-with-access-to-both-storage-accounts

Ask our Experts

Did you like this **Question?**

Question 6 Incorrect

Domain: Implement and manage storage

Which feature should Contoso enable to protect against accidental deletions or modifications of blobs in Azure Blob Storage?

A. Azure Storage firewalls and virtual networks

B. Blob encryption wrong

C. Blob versioning right

D. Azure Backup

Explanation:

Correct Answer: C

Option C is CORRECT because blob versioning automatically maintains previous versions of blobs when they are modified or deleted, allowing users to restore earlier versions if necessary. This feature directly addresses the requirement to protect against accidental deletions or modifications by retaining historical versions of blobs. Enabling blob versioning would allow Contoso to recover data in case of errors or unintended changes.

Option A is INCORRECT because Azure Storage firewalls and virtual networks help control access to Azure Storage accounts by restricting access based on IP address ranges and virtual network configurations. This feature enhances security by limiting who can access the storage account, but it does not directly address protecting against accidental deletions or modifications of blobs.

Option B is INCORRECT because blob encryption ensures that the data stored in Azure Blob Storage is encrypted at rest, providing an additional layer of security. While encryption is crucial for protecting data confidentiality, integrity, and compliance, it doesn't directly address the need for maintaining previous versions of blobs for recovery purposes.

Option D is INCORRECT because Azure Backup is a service that allows organizations to back up data from on-premises systems and Azure services to Azure Storage. While Azure Backup is valuable for data protection and disaster recovery, it is not specifically designed for protecting blobs against accidental deletions or modifications. Azure Backup focuses more on regular backups and restoring entire systems or datasets, rather than managing versioning at the blob level.

Reference:

https://learn.microsoft.com/en-us/azure/storage/blobs/versioning-enable?tabs=portal

Ask our Experts

Did you like this **Question?**

Question 7 Correct

Domain: Implement and manage storage

Contoso wants to ensure that only authorized users from their corporate network (10.0.0.0/16) and a specific Azure virtual network (VNet1) can access their Azure Blob Storage account. Which configuration option should they use to achieve this?

A. Azure Storage firewalls and virtual networks right

B. Blob encryption

C. Blob versioning

D. Azure Backup

Explanation:

Correct Answer: A

Option A is CORRECT because Azure Storage firewalls and virtual networks help control access to Azure Storage accounts by restricting access based on IP address ranges and virtual network configurations. It can allow Contoso to control access to their Azure Blob Storage account based on IP address ranges and Azure Virtual Network configurations. Contoso can specify allowed IP addresses or IP address ranges, including their corporate network (10.0.0.0/16), and configure access permissions for specific Azure Virtual Networks like VNet1. This option aligns with Contoso's requirement to restrict access to their storage account to authorized users from their corporate network and a specific Azure Virtual Network.

Option B is INCORRECT because blob encryption ensures that the data stored in Azure Blob Storage is encrypted at rest, providing security for the stored data. While encryption is important for protecting data confidentiality, integrity, and compliance, it does not directly control access to the storage account based on IP addresses or virtual networks.

Option C is INCORRECT because blob versioning automatically maintains previous versions of blobs when they are modified or deleted, allowing users to restore earlier versions if necessary. While blob versioning is essential for data protection and recovery, it does not control access to the storage account based on IP addresses or virtual networks.

Option D is INCORRECT because Azure Backup is a service that allows organizations to back up data to Azure Storage for data protection and disaster recovery purposes. While Azure Backup is valuable for backing up and restoring data, it does not control access to Azure Blob Storage based on IP addresses or virtual networks.

Reference:

Configure Azure Storage firewalls and virtual networks | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 8

Incorrect

Domain: Implement and manage storage

As part of their data migration strategy, Contoso needs to transfer large datasets from their on-premises systems to Azure Blob Storage. Which tool should they utilize to perform this task efficiently and maintain data integrity?

A. Azure Storage Explorer

B. Azure Data Box right

C. Azure Data Factory

D. AzCopy wrong

Explanation:

Correct Answer: B

When transferring large datasets from on-premises to Azure Blob Storage, Azure Data Box is the most efficient and reliable tool for the job.

Designed for large-scale data transfers (terabytes to petabytes).
Provides a secure, ruggedized physical device that you load data onto locally.
Microsoft then ships the device back, and the data is uploaded directly into your Azure Blob Storage.
Ensures data integrity and encryption throughout the process.

Option A is INCORRECT because while Azure Storage Explorer helps explore and manage data within Azure storage accounts, it may not be the most efficient tool for transferring large datasets from on-premises systems to Azure Blob Storage, especially when dealing with huge volumes of data.

Option C is INCORRECT because Azure Data Factory supports hybrid data integration, enabling users to efficiently transfer data between on-premises systems and cloud storage services like Azure Blob Storage. Azure Data Factory is well-suited for orchestrating complex data workflows and handling large datasets.

Option D is INCORRECT. Command-line tool for fast uploads/downloads to Blob Storage. Works well for moderate-sized datasets, but not ideal for very large volumes due to bandwidth and time constraints.

Reference:

Tutorial: Migrate on-premises data to Azure Storage with AzCopy | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 9

Correct

Domain: Implement and manage storage

You have an Azure subscription. You created a storage account in the EastUS location and a virtual machine in the WestUS location and integrated both the services for a common requirement. What should you configure on the storage account to ensure that data moving between the storage account and the virtual machine does not go over the internet?

A. Data protection

B. A private endpoint right

C. A shared access signature (SAS)

D. None of the above

Explanation:

Correct Answer: B

Option B is CORRECT because a private endpoint allows you to connect privately to a service powered by Azure Private Link. It provides secure connectivity between the virtual network and the Azure service, such as Azure Storage. By configuring a private endpoint for the storage account, you can ensure that data transfers occur securely within the Azure network and do not traverse the internet.

Option A is INCORRECT because data protection typically refers to measures taken to safeguard data integrity, confidentiality, and availability. While important, it does not directly address the requirement to ensure that data transfers between the storage account and virtual machine do not traverse the internet.

Option C is INCORRECT because a Shared Access Signature (SAS) provides secure delegated access to resources in a storage account without sharing the account keys. While SAS tokens can help control access to resources, they do not inherently prevent data transfers between the storage account and virtual machine from going over the internet.

Option D is INCORRECT because this option implies that there is another solution or configuration that should be implemented to achieve the requirement of ensuring that data transfers between the storage account and virtual machine do not traverse the internet. However, given the context of the question, option B, configuring a private endpoint, would be the appropriate choice.

Reference:

https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

Ask our Experts

Did you like this **Question?**

Question 10

Correct

Domain: Implement and manage storage

You have an Azure subscription. The subscription contains a list of devices along with the platforms configured as shown in the below exhibit:

DEVICE NAME	PLATFORM
Device1	Windows
Device2	Ubuntu Linux

Device3	Android
Device4	macOS

Which device(s) can be used to install Azure Storage Explorer?

A. Device1 only

B. Device1 and Device3 only

C. Device1, Device2 and Device4 only right

D. Device1, Device2 and Device3 only

Explanation:

Correct Answer: C

Option C is CORRECT because Azure Storage Explorer is available for Windows, macOS, and Linux. Device1 runs on Windows, Device2 runs on Ubuntu Linux, and Device4 runs on macOS, all of which are supported platforms for Azure Storage Explorer. Therefore, Device1, Device2, and Device4 can be used to install Azure Storage Explorer.

Option A is INCORRECT because Device1 is running on Windows, which is a supported platform for Azure Storage Explorer. So, it is possible to install Azure Storage Explorer on Device1. This option is partially correct as it identifies one device correctly, but it neglects other devices that also support Azure Storage Explorer.

Option B is INCORRECT because Device3 runs on Android, which is not a supported platform for Azure Storage Explorer.

Option D is INCORRECT because Device3 runs on Android, which is not a supported platform for Azure Storage Explorer.

Reference:

Get started with Storage Explorer | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 11

Incorrect

Domain: Implement and manage storage

You create an Azure storage account and add a file share.

Please select steps that you need to implement for secure access to the Azure files from on-premises.

- [x] A. Enable port 445 right
- [ ] B. Create service principal
- [x] C. Create a firewall rule based on IP client access right
- [ ] D. Secure transfer required right
- [x] E. Enable port 3389 wrong

Explanation:

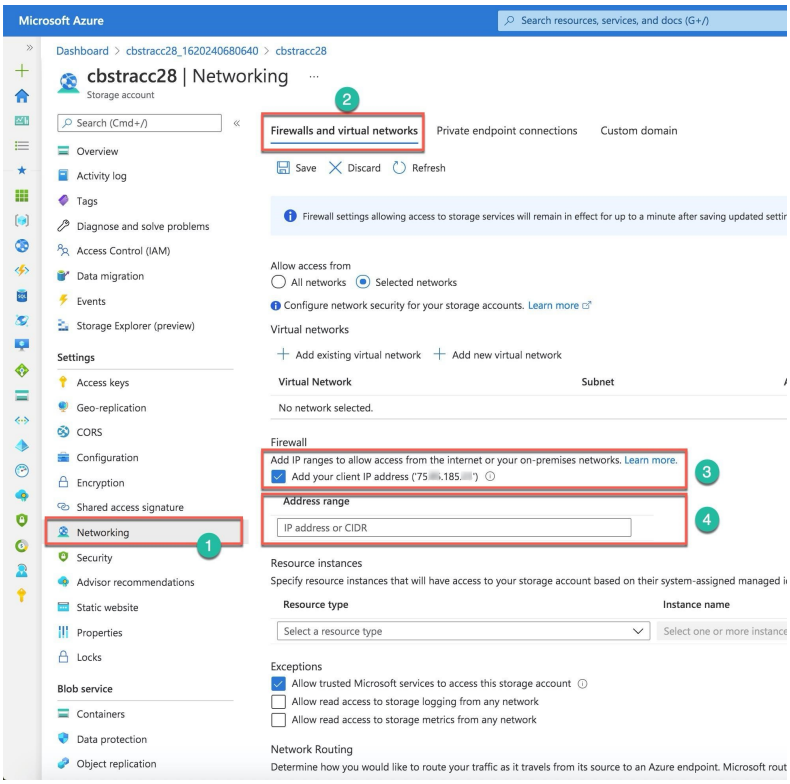
Correct Answers: A, C, and D

Option B is incorrect because the service principal is an identity for applications and services to access Azure resources, and it is irrelevant to the file share access.

Option E is incorrect because port 3389 is an RDP port, and it is irrelevant to the file share access.

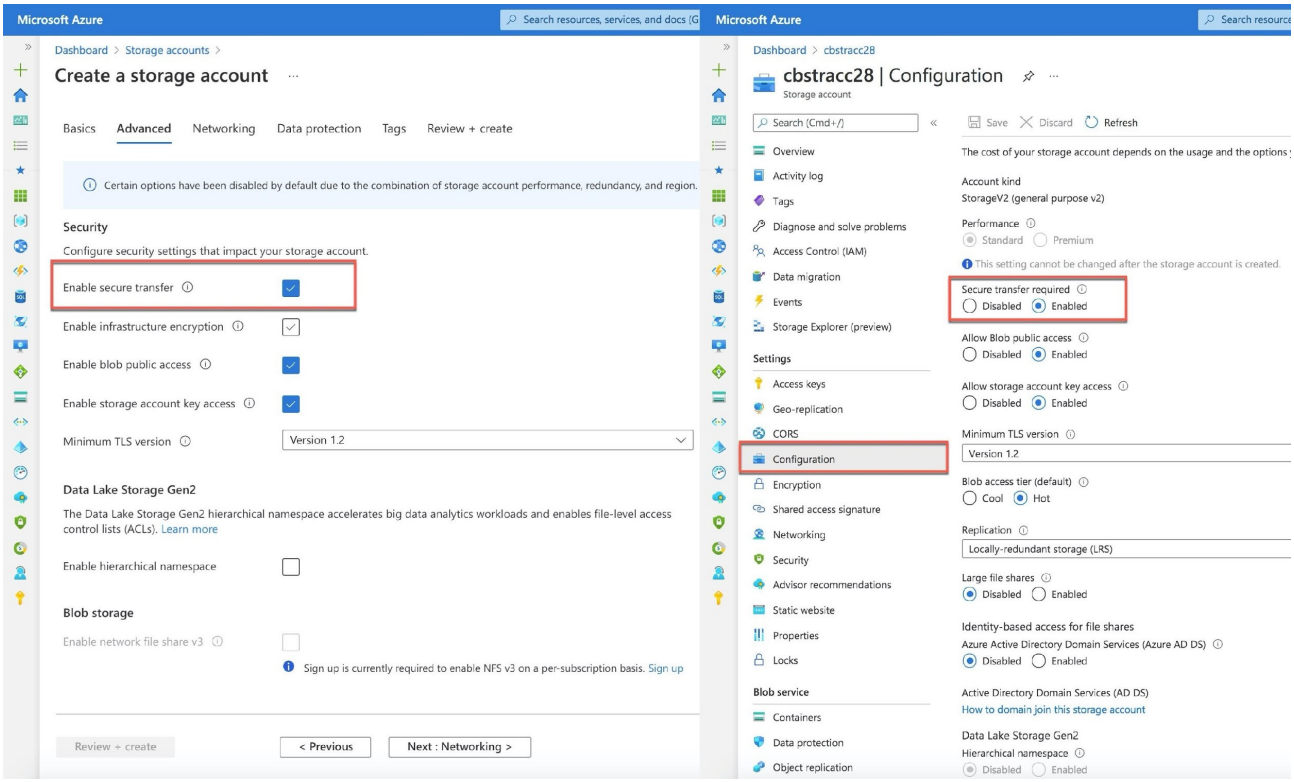
To secure access to shared Azure Files from on-premises, you need to ensure that your SMB port 445 is enabled. Users can access the Azure Files using the Server Message Block (SMB) or Network File System (NFS) protocols.

Clients can access the SMB file shares on Windows, Linux, or macOS. The NFS protocol applies to Linux and macOS clients. The secure way of accessing the files when you know the incoming IP address of the client. On the Networking screen for the storage account (Number 1), you can create an Azure storage firewall rule (Number 2) based on the known client IP address (Number 3) or the address range (Number 4) and limit access to the files.

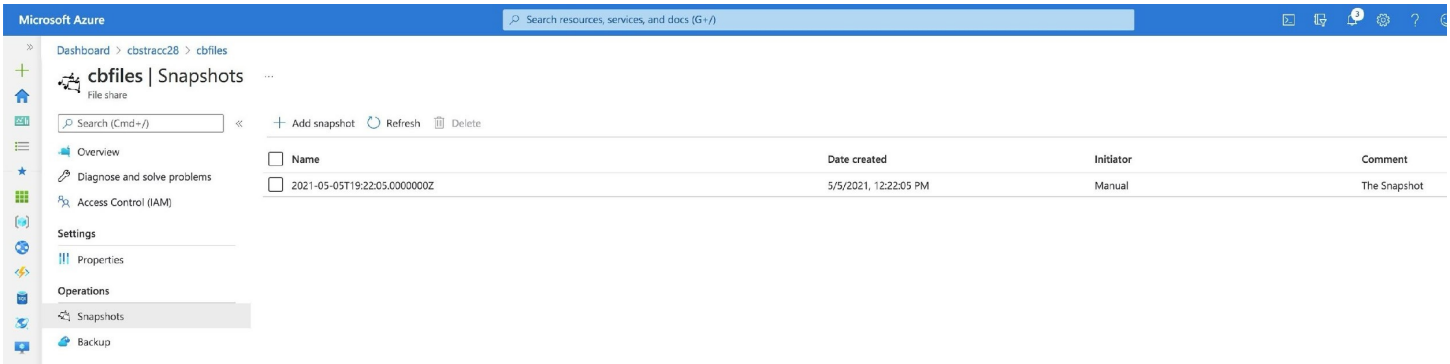


You need to require the secure transfer when you create a storage account (Number 1) or enable this option (Number 3) on the Configuration screen (Number 2). It will force REST clients to establish only HTTPS connections and reject not secure data transfer

when using SMB protocol.



To prevent accidental deletion of the files, you need to use the Share snapshots of your file shares, the backups, and soft deletes.



For more information about secure access to file shares, please visit the below URLs:

https://docs.microsoft.com/en-us/learn/modules/store-and-share-with-azure-files/5-secure-azure-files

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#managing-virtual-network-rules

Ask our Experts

Did you like this **Question?**

Question 12 Correct

Domain: Implement and manage storage

View Case Study

In the planned changes, move the existing business critical data from File Servers to Azure Files. The file servers are migrated to Azure files.

Share name: \\azfs.file.core.windows.net\Data

Which of the following identity types would you use to manage share level permissions and file/directory level permission?

Your Answers

Authenticating to Azure file shares.

AD DS authentication

Windows Access Control List

File/Directory Level Permissions

Microsoft Entra ID users or groups

Share Level Permissions

Correct Answers

Authenticating to Azure file shares.

AD DS authentication

Windows Access Control List

File/Directory Level Permissions

Microsoft Entra ID users or groups

Share Level Permissions

Explanation:

Correct Answer: 1-A, 2-C, 3-B

Authenticating to Azure file shares: AD DS authentication

Windows Access Control List: File/Directory Level Permissions

Microsoft Entra users or groups: Share Level Permissions

Active Directory Domain Services (AD DS) authentication allows you to use your on-premises AD credentials to access Azure file shares. This means you can manage permissions using the same identities and groups you already have in your AD environment. This setup provides a seamless integration with your existing identity infrastructure.

File and directory-level permissions in Azure Files are managed using Windows Access Control Lists (ACLs). These permissions allow you to control access at a more granular level, specifying what operations users can perform on individual files or directories. For example, you can set read, write, or modify permissions for specific users or groups. These permissions are enforced alongside share-level permissions, with the most restrictive permission taking precedence

Share-level permissions determine whether a user can access the entire file share. These permissions are typically managed using Azure Role-Based Access Control (RBAC), which allows you to assign roles to Microsoft Entra (formerly Azure AD) users, groups, or

service principals. Share-level permissions act as a high-level gatekeeper, and you must configure these before setting more granular file/directory-level permissions.

References:

Control what a user can do at the directory and file level - Azure Files

Enable AD DS authentication for Azure file shares | Microsoft Learn

Control access to Azure file shares by assigning share-level permissions | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 13

Incorrect

Domain: Implement and manage storage

A multinational company has a storage account named “mncstore”.

The communication between a client application and the storage account is encrypted using Transport Layer Security (TLS). Which of the following TLS version is not supported by the azure storage account?

A. 1.0 wrong

B. 1.1

C. 1.2

D. 1.3 right

Explanation:

Correct Answer: D

Azure Storage currently supports three versions of the TLS protocol: 1.0, 1.1, and 1.2. Azure Storage uses TLS 1.2 on public HTTPS endpoints, but TLS 1.0 and TLS 1.1 are still supported for backward compatibility.

Option A is incorrect because 1.0 is supported for backward compatibility of previous version of TLS that is now deprecated for most of the applications.

Option B is incorrect because 1.1 is still supported for the legacy applications.

Option C is incorrect because azure storage uses the 1.2 version for TLS public endpoints.

Option D is correct because it is not supported by the azure storage account at the moment.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/transport-layer-security-configure-minimum-version?tabs=portal

Ask our Experts

Did you like this **Question?**

Question 14 Incorrect

Domain: Implement and manage storage

A multinational company has hired an external auditor. You as a security engineer are tasked to grant access to storage accounts for a limited period of time. Which of the following solutions is the best way to grant permission to the external auditor?

A. Shared storage access key

B. Permission through Access Control

C. Shared Access Signature right

D. Group Policy wrong

Explanation:

Correct Answer: C

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources for a specified period of time, with a specified set of permissions. You can provide a shared access signature to clients who should not be trusted with your storage account key but to whom you wish to delegate access to certain storage account resources.

Option A is incorrect because when you create a storage account, Azure generates two 512-bit storage account access keys for that account. These keys can be used to authorize access to data in your storage account via Shared Key authorization.

Option B is incorrect because You can associate a security principle with an access level for files and directories. Each association is captured as an entry in an access control list (ACL). Each file and directory in your storage account has an access control list.

Option C is correct because A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources for a specified period of time, with a specified set of permissions.

Option D is incorrect because Group Policies can be used to grant access to file shares.

Reference:

https://docs.microsoft.com/en-us/rest/api/storageservices/delegate-access-with-shared-access-signature

Ask our Experts

Did you like this **Question?**

Question 15 Correct

Domain: Implement and manage storage

A company is planning to migrate its on-premises files data to Azure. They have a storage account named 'mystorageunit'. The company wants to ensure that data is encrypted at rest using the company's provided keys.

Which of the following services supports such requirements? (Select Two)

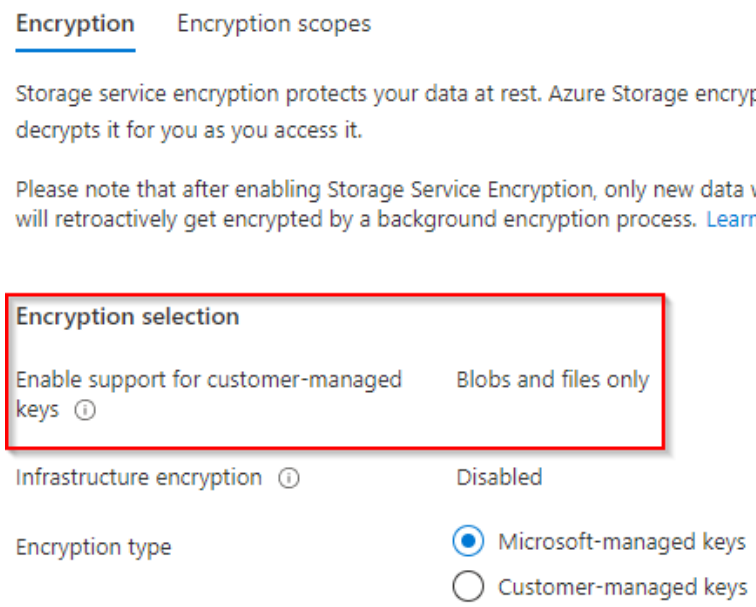
- [x] A. Azure Files right
- [ ] B. Azure Table storage
- [x] C. Azure Blob storage right
- [ ] D. Azure Queue storage

Explanation:

Correct Answers: A and C

Azure Storage by default encrypts all data in a storage account at rest. By default, data is encrypted with Microsoft-managed keys. Customer-managed keys rely on managed identities for Azure resources, a feature of Microsoft Entra ID. Managed identities do not currently support cross-tenant scenarios. When you configure customer-managed keys in the Azure portal, a managed identity is automatically assigned to your storage account under the covers. If you subsequently move the subscription, resource group, or storage account from one Microsoft Entra ID tenant to another, the managed identity associated with the storage account is not transferred to the new tenant, so customer-managed keys may no longer work.

Option A is correct because by design Customer-managed key (CMK) support can be limited to blob service and file service only. Once the storage account is created, this support cannot be changed.



Option B is incorrect because data stored in Table storage is not automatically protected by a customer-managed key when customer-managed keys are enabled for the storage account, however, it can be configured during the time of the creation of the storage account.

Option C is correct because by design Customer-managed key (CMK) support can be limited to blob service and file service only. Once the storage account is created, this support cannot be changed.

The following table compares key management options for Azure Storage encryption.

Key management parameter	Microsoft-managed keys	Customer-managed keys	Customer-provided keys
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob Storage, Azure Files[1,2]	Blob Storage
Key storage	Microsoft key store	Azure Key Vault or Key Vault HSM	Customer's own key store

Option D is incorrect because data stored in Queue storage is not automatically protected using customer-managed keys, however, it can be configured during the time of storage account creation.

References:

Configure customer-managed keys for an existing storage account - Azure Storage | Microsoft Docs

Azure Storage encryption for data at rest | Microsoft Docs

Ask our Experts

Did you like this **Question?**

Finish Review