A screenshot of a computer

AI-generated content may be incorrect.

There are three ways to implement identity-based authentication over SMB: **On-Premises Active Directory Domain Services (AD DS), Microsoft Entra Domain Services, Microsoft Entra Kerberos (hybrid identities only)**

1. AD DS clients and Virtual Machines can access Azure file shares with **on-premises Active Directory** credentials. The AD must be synced to Entra ID with Entra Connect application or Entra Connect cloud sync
2. Entra Kerberos for hybrid identities can use Entra ID to authenticate hybrid user identities, allowing end users to access Azure file shares without network connectivity to **domain controllers** (that’s for hybrid connections ONLY – cloud-only identities aren’t supported using this method)

A screenshot of a computer

AI-generated content may be incorrect.

The answer is self-explanatory. However, not only can file shares be retained for 365 days, but data in them can also be retained.

A screen shot of a computer

AI-generated content may be incorrect.

AzCopy is a tool provided by Microsoft for copying data to or from Blob Storage, Azure Files **AND** Table Storage. Designed for high-performance data transfer especially where automation and scripting is required

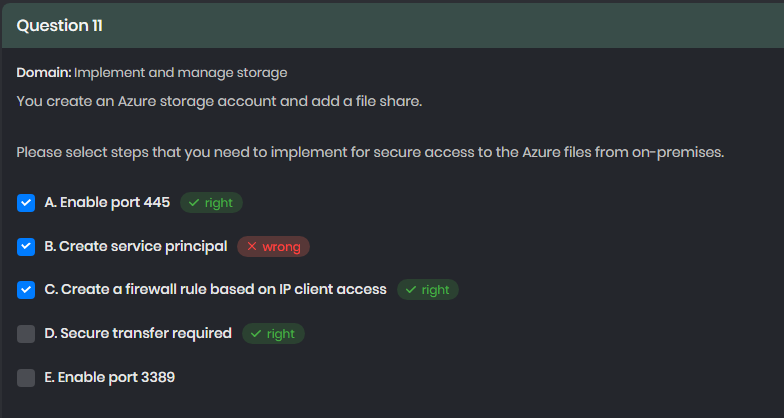
DataBox in this case is incorrect, because it’s more suitable where transferring data over the network may be impractical due to bandwidth limitations or large dataset sizes. Besides doing the job, it requires the physical ship of the appliance to the customer’s location

DataFactory also transfer data from on-prem to Cloud, but that’s a transformation tool (it does ETL/ELT, in fact)

A screenshot of a computer

AI-generated content may be incorrect.

Azure Storage Explorer is available for Windows, Linux and MacOS



There are two ways of doing secure, and both should probably be executed:

1. Go to networking and set a firewall rule, in this case, the IP address or CIDR block range of the on-prems network
2. Go to configuration and Enable Secure transfer. It will force REST clients to establish only HTTPS connections

A screenshot of a computer

AI-generated content may be incorrect.

AD DS allows you to use on-prems AD credentials to access azure file shares. You can manage permissions using the same identities and groups you already have in your AD env.

File and directory-level permissions in Azure Files are managed by Windows ACLs – probably the mounted network drive can be managed as any other

Share-level permissions are typically managed using Azure RBAC, which allows to assign roles to Entra users, groups, or service principals. This is a high-level gatekeeper and must be set before the files/directory level permissions, which performs more granular control over the permissions of a principal

1. Entra ID for authentication
2. Share-Level Permissions
3. Directory/File-Level Permissions

[https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions](https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal)

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-configure-file-level-permissions>

A screenshot of a computer

AI-generated content may be incorrect.

1.3 is not supported at the moment and 1.0 is supported for backward compatibility