

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. Some nodes are highlighted with blue circles, and others with solid blue dots.

Data Security

Storage Security

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, with interconnected nodes and lines, some highlighted with blue circles and others with solid blue dots.

A decorative graphic in the top-left corner consisting of a network of interconnected nodes and lines, rendered in a light gray color. The nodes are represented by small circles, some of which are solid and others are hollow, connected by thin lines.

Hello!

I am Eng Teong Cheah

Microsoft MVP

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or central structure. The lines are thin and gray, connecting the nodes in a non-linear fashion.

Data Security

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes being larger and more prominent than others. The overall style is clean and modern, using a light gray color scheme.

Data Sovereignty

- ◎ The concept that information which has been converted and stored in binary digital form is subject to the laws of the country or region in which it is located.
- ◎ In Azure, customer data might be replicated within a selected geographic area for enhanced data durability in case of a major data center disaster, and in some cases will not be replicated outside it.

Azure Storage Access

Storage	Storage Account Share Key	Shared access signature	Azure Active Directory	Active Directory (preview)	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not Supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with Azure AD Domain Services	Supported, credentials must be synced to Azure AD	Not Supported
Azure Files (REST)	Supported	Supported	Not Supported	Not supported	Not supported

Shared Access Signatures

- ◎ Digitally signed URIs of target storage resources
- ◎ Grants access to clients without sharing your storage account keys
- ◎ Two SAS types: Account and Service
- ◎ Configure permissions, start/expiry times, IP address, and allowed protocols

Azure AD Storage Authentication

- ◎ Authorization with Azure AD is available for all general-purpose and Blob storage accounts in all public regions and national clouds.
- ◎ Built-in storage roles are provided including Owner, Contributor, and Reader.
- ◎ The role can be scoped from Management Group to individual blob or queue. Best practices dictate granting only the narrowest possible scope.

Azure AD Storage Authentication

- ◎ RBAC role assignments may take up to five minutes to propagate.

Blob Data Retention Policies

- ◎ Data recovery and disposal rules
- ◎ Time-based retention for a specified interval (days)
- ◎ Legal-hold retention based on tags – no editing or deleting of the content
- ◎ Container policies apply to all existing and new content
- ◎ Supports audit logging

Azure Files Authentication

- ◎ Enable identity-based authentication
- ◎ Use Azure AD DS or on-premises AD DS (preview)
- ◎ Use RBAC roles to assign access rights to the file shares
- ◎ Enforces standard Windows file permissions at both the directory and file level

Secure Transfer Required

- ◎ Storage account connections must be secure (HTTPS)
- ◎ HTTPS for custom domain names not supported
- ◎ Azure Files connections require encryption (SMB)

Demonstrations

Service Endpoints and Securing Storage



Thanks!

Any questions?

You can find me at:
[@walkercet](#)

References

© <https://docs.microsoft.com/en-us/>