ThreatModel for Azure Storage

Introduction

Read the blog: The last Azure Storage security document that we'll ever need.

Content

This publication includes:

- overall data flow diagram of Azure Storage

- overview of the Mitre ATT&CK matrix for Azure Storage

- prioritized list of all threat scenarios

- list of all the control activities and testing procedures

- risk-based prioritized list of control implementation

License Agreement

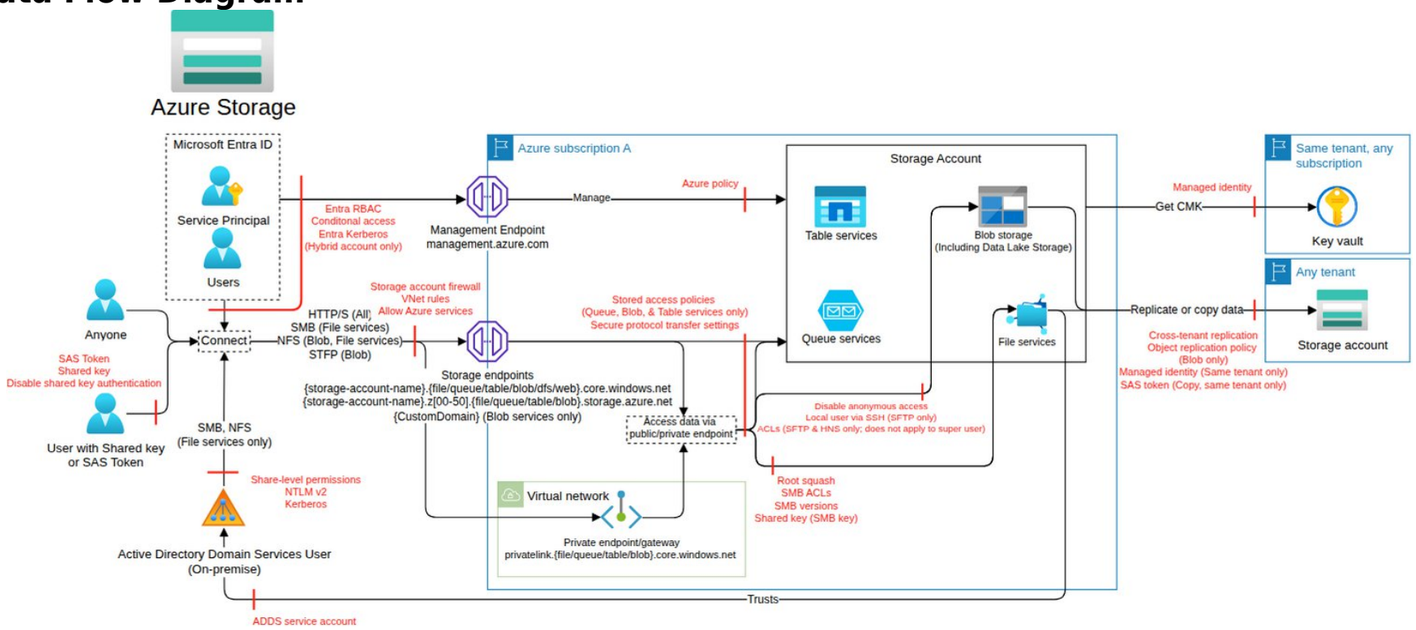
Source

The latest version of this work is hosted on GitHub.

Contact

If you have any questions, please contact chatbot@trustoncloud.com.

Data Flow Diagram



Security Scorecard

Security in the Cloud	
Number of Actions*	184
Identity management	Azure RBAC, storage account key, local SFTP users, Entra ID, AD DS, Azure AD Kerberos
Number of IAM permissions*	139
Resource-based access	file share ACL, queue ACL, table ACL, storage account access keys, SAS tokens
Logging coverage for APIs	60.1% (missing 63)
Number of Logging Event Names*	109
Network Filtering	VNET security, Storage Account Firewall, Private endpoint
Encryption-at-rest	Yes
Encryption-in-transit	Yes

* See details in Appendixes

Mitre ATT&CK matrix for Azure Storage

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		File share access through SMB Shared Key [Storage.T65]	Distribute malicious data by using the storage account name [Storage.T4]	Execution of malware through file replacement [Storage.T12]	Unauthorized data exposure by modifying CORS settings [Storage.T26]	Defense evasion by modifying diagnostic settings [Storage.T10]	Credential access through accessing SMB Shared Key [Storage.T64]					Privilege escalation using storage account access key [Storage.T1]	DoS due to storage account access key regeneration [Storage.T2]
				Distribute malicious files via file share [Storage.T20]	Privilege escalation by modifying queue access policy [Storage.T27]							Unauthorized access to data by allowing anonymous public access [Storage.T5]	Recursively delete DFS directories and their content [Storage.T7]
					Privilege escalation by modifying table access policy [Storage.T28]							Unauthorized access to data via storage account replication [Storage.T13]	Unauthorized modification of data [Storage.T8]
					Service compromise by disabling soft delete [Storage.T39]							Exfiltrate data using different access methods [Storage.T15]	Encrypt/overwrite files with ransomware in DFS/blob [Storage.T9]
					Privilege escalation through modification of ACL [Storage.T66]							Exfiltrate files via the static website feature [Storage.T22]	Denial of Wallet (DoW) through the upload of files to a storage account [Storage.T16]
												Exfiltrate metadata using blob inventory functionality [Storage.T24]	Recursively delete directories and their contents in the file share [Storage.T18]
												Persistent access to data by creating SFTP local user credentials [Storage.T44]	Delete data using Blob Storage lifecycle management [Storage.T25]
												Information disclosure due to unencrypted blob storage [Storage.T49]	Impacting queue's message integrity or complete loss of sensitive data [Storage.T31]
												Access to Storage account resources by modifying virtual network rules [Storage.T50]	Cost increase by executing Azure Data Lake Storage query acceleration [Storage.T34]
												Data exposure by changing encryption type [Storage.T60]	Data integrity failure by tampering with encryption-at-rest key [Storage.T38]
												Data exposure through exploitation of legacy protocols [Storage.T61]	Denial of Service by removing replication [Storage.T42]
												Exfiltration through rogue replication policy [Storage.T63]	Unauthorized failover through configuration change [Storage.T59]
													Denial of Service by deleting private endpoint [Storage.T62]

Feature Classes

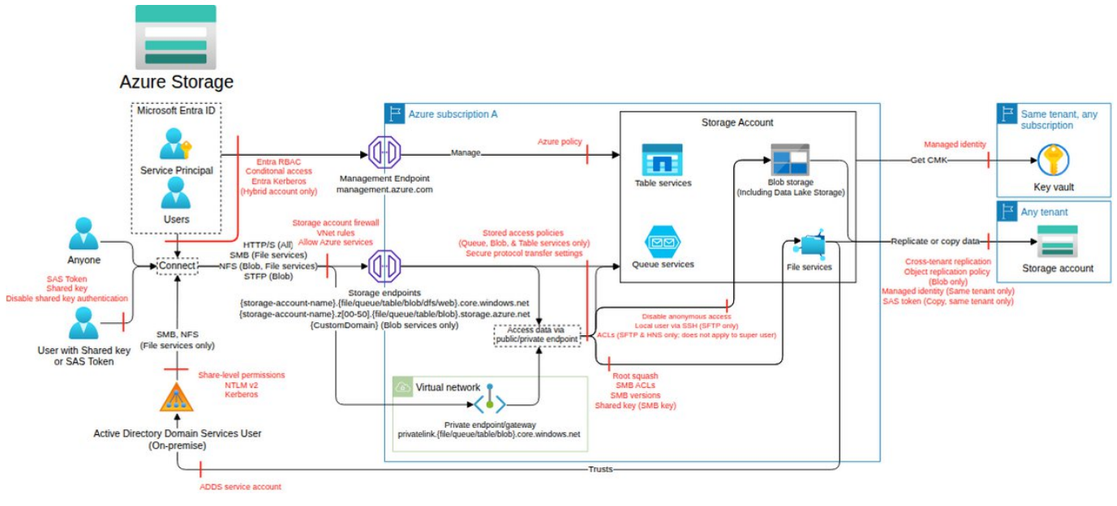
Azure Storage has the following feature classes and subclasses (i.e. dependent on the usage of its class) that can be activated, restricted, or blocked using Microsoft Azure Identity and Access Management.

Feature	Relation	Description
Storage account (FC1)	class	Azure Storage is Microsoft's Cloud Storage solution for modern data storage scenarios. Azure Storage offers a scalable object store for data objects, a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store.
Blob storage (FC2)	subclass of Storage account	Object storage solution for storing unstructured data (blobs) accessible via HTTP/S and optionally via the Network File System (NFS) v3 and SFTP protocols.
Blob inventory (FC10)	subclass of Blob storage	The Azure Storage blob inventory feature provides an overview of your containers, blobs, snapshots, and blob versions within a storage account. Use the inventory report to understand various attributes of blobs and containers, such as the total data size, age, encryption status, immutability policy, and legal hold.
File shares (FC3)	subclass of Storage account	Azure Files offers fully governed file shares in the cloud accessible via Server Message Block (SMB) protocol, Network File System (NFS) v4.1 protocol, or the in-preview Azure Files REST API.
Queues (FC4)	subclass of Storage account	Azure Queue Storage is a service for storing messages. Access messages via HTTP/S calls.
Tables (FC5)	subclass of Storage account	Azure table storage is a service that stores non-relational structured data (or structured NoSQL data) in the cloud, providing a key/attribute store with a schemaless design.
Local users (FC11)	subclass of Storage account	Blob storage supports the SSH File Transfer Protocol (SFTP). This support lets you securely connect to blob storage via an SFTP endpoint, allowing you to use SFTP for file access, file transfer, and file management.
Private endpoints (FC12)	subclass of Storage account	Azure Storage private endpoint is a network interface that enables secure, private connectivity between Azure Storage and virtual networks using Azure Private Link, preventing exposure to the public internet and enhancing security.

Storage account *(class, FC1)*

Azure Storage is Microsoft's Cloud Storage solution for modern data storage scenarios. Azure Storage offers a scalable object store for data objects, a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

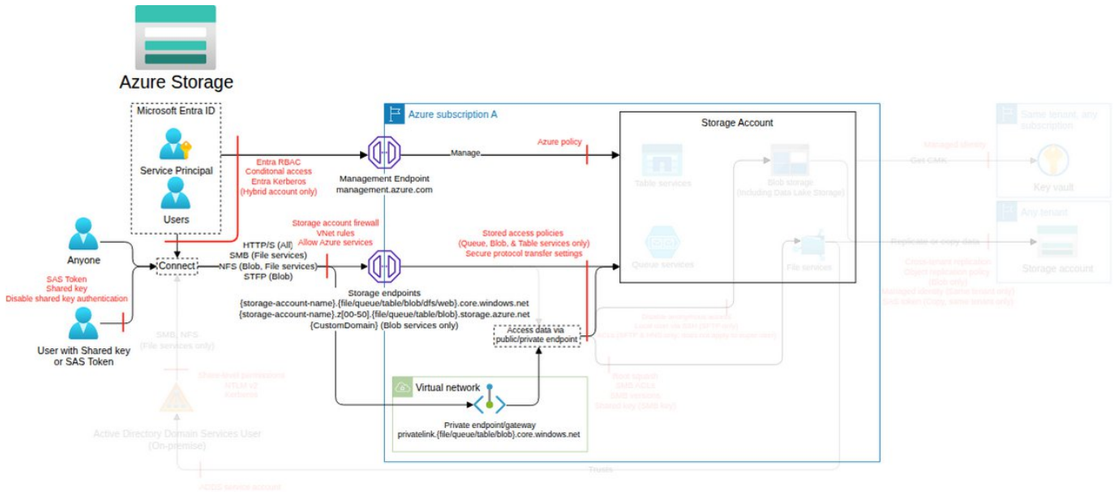
Action	IAM Permission
Asynchronously creates a new storage account with the specified parameters. If an account is already created and a subsequent create request is issued with different properties, the account properties will be updated. If an account is already created and a subsequent create or update request is issued with the exact same set of properties, the request will succeed. The update operation can be used to update the SKU, encryption, access tier, or tags for a storage account.	Microsoft.Storage/storageAccounts/write

Threat List

Name	CVSS
Privilege escalation using storage account access key	High (8.1)
Data integrity failure by tampering with encryption-at-rest key	Medium (5.7)
Exfiltration through rogue replication policy	Medium (5.6)
Distribute malicious data by using the storage account name	Medium (5.2)
Delete data using Blob Storage lifecycle management	Medium (5.2)
Service compromise by disabling soft delete	Medium (5.2)
Denial of Service by removing replication	Medium (5.2)
Unauthorized access to data via storage account replication	Medium (5.2)
DoS due to storage account access key regeneration	Medium (4.5)
Unauthorized data exposure by modifying CORS settings	Medium (4.0)
Unauthorized failover through configuration change	Low (3.5)
Information disclosure due to unencrypted blob storage	Low (3.5)
Access to Storage account resources by modifying virtual network rules	Low (3.4)
Defense evasion by modifying diagnostic settings	Low (2.4)

Privilege escalation using storage account access key

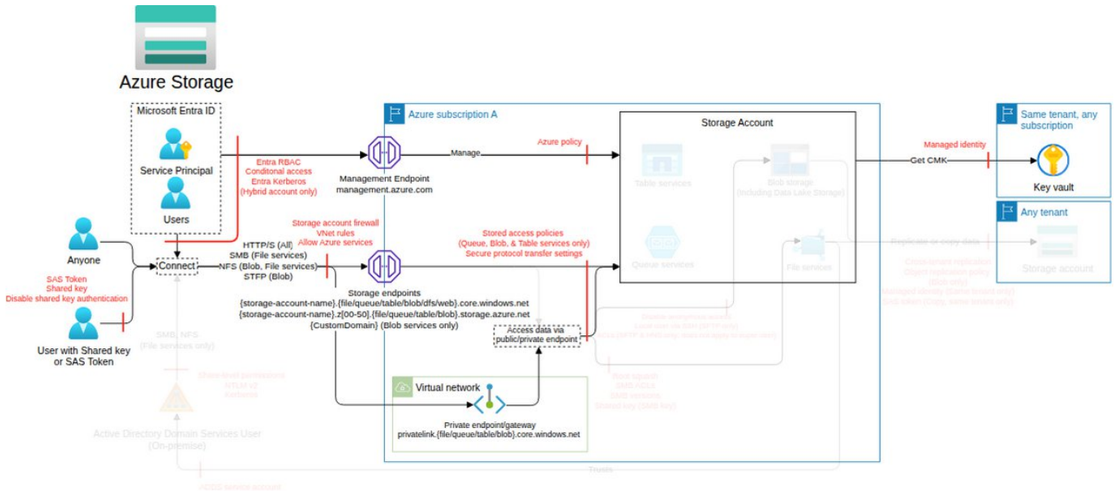
Threat Id	Storage.T1
Name	Privilege escalation using storage account access key
Description	Storage accounts can have up to 2 storage access keys with unrestricted permissions on a storage account. An attacker can generate a new storage access key or use an existing key to gain unrestricted access.
Goal	Launch another attack
MITRE ATT&CK®	TA0010
CVSS	High (8.1)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/listKeys/action", "Microsoft.Storage/storageAccounts/regenerateKey/action", "Microsoft.Storage/storageAccounts/rotateKey/action"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts. C42 - Maintain a list of authorized IPs that are permitted through each storage account firewall. C43 - Ensure each storage account firewall only allows authorized IPs. C44 - Prevent access from unauthorized IPs by allowing only authorized IPs through the Azure Storage firewall (by using built-in Azure Policy "Storage accounts should restrict network access" in Deny mode).	Very High	4	1	-

Data integrity failure by tampering with encryption-at-rest key

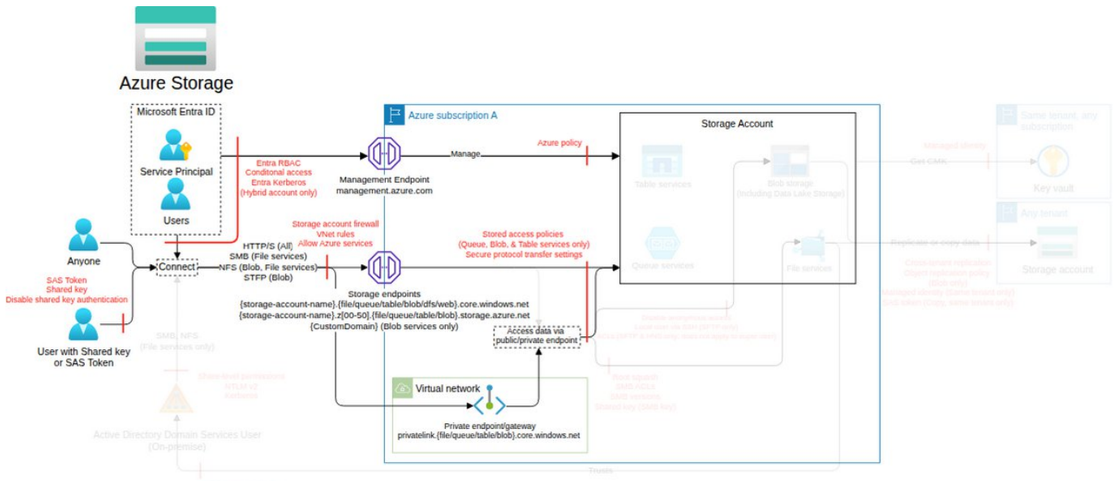
Threat Id	Storage.T38
Name	Data integrity failure by tampering with encryption-at-rest key
Description	Data at rest can be encrypted with customer managed keys. An attacker can change the encryption key, causing a data integrity failure.
Goal	Disruption of Service
MITRE ATT&CK®	TA0040
CVSS	Medium (5.7)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/encryptionScopes/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO12 - Enforce encryption on data at rest and protect encryption keys C60 - Maintain a list of authorized customer-managed keys used by storage accounts. C61 - Ensure only authorized customer-managed keys are configured for storage accounts. C63 - Prevent storage accounts that require customer-managed keys from using service-managed keys (e.g., by using built-in Azure Policy "Storage accounts should use customer-managed key for encryption" in Deny mode).	High	2	1	-

Exfiltration through rogue replication policy

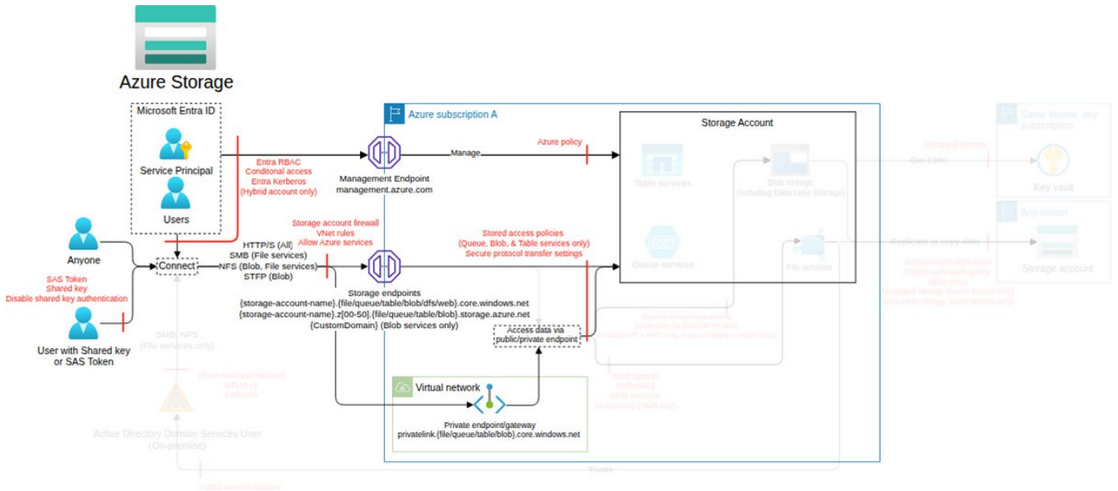
Threat Id	Storage.T63
Name	Exfiltration through rogue replication policy
Description	Replication policies allow continuous replication of objects (files, blobs, etc.). An attacker can set up a rogue replication policy to continuously replicate objects to a storage account they control, including being located in an external tenant.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Medium (5.6)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C107 - Maintain the list of storage accounts that should require read-only and/or delete locks. C108 - Ensure only required storage accounts have read-only and/or delete locks applied. C110 - Prevent modification or deletion of required storage accounts by using a resource lock set to read-only and/or delete, using the Azure Resource Manager ThreatModel.	Very High	2	1	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C47 - Maintain a list of storage accounts that require cross-tenant replication and their allowed destination tenants. C48 - Ensure only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized.	Very High	2	-	-

Distribute malicious data by using the storage account name

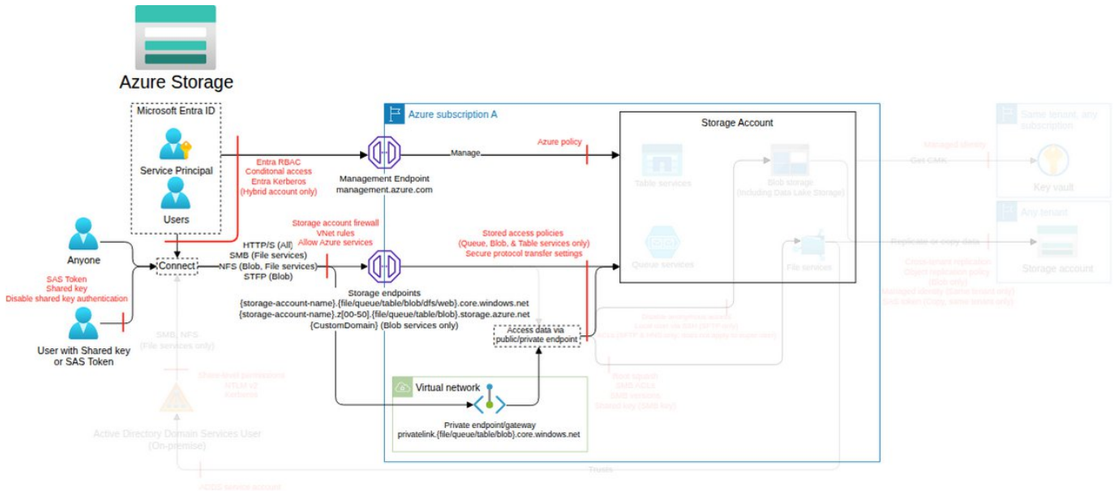
Threat Id	Storage.T4
Name	Distribute malicious data by using the storage account name
Description	Azure Storage account names are globally unique. An attacker can take over an old or existing account name, delete one, and trick any third party to use their account to steal or distribute malicious data.
Goal	Data manipulation
MITRE ATT&CK®	TA0002
CVSS	Medium (5.2)
IAM Access	{ "OPTIONAL": "Microsoft.Storage/storageAccounts/delete" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C107 - Maintain the list of storage accounts that should require read-only and/or delete locks. C108 - Ensure only required storage accounts have read-only and/or delete locks applied.	Very High	2	-	-

Delete data using Blob Storage lifecycle management

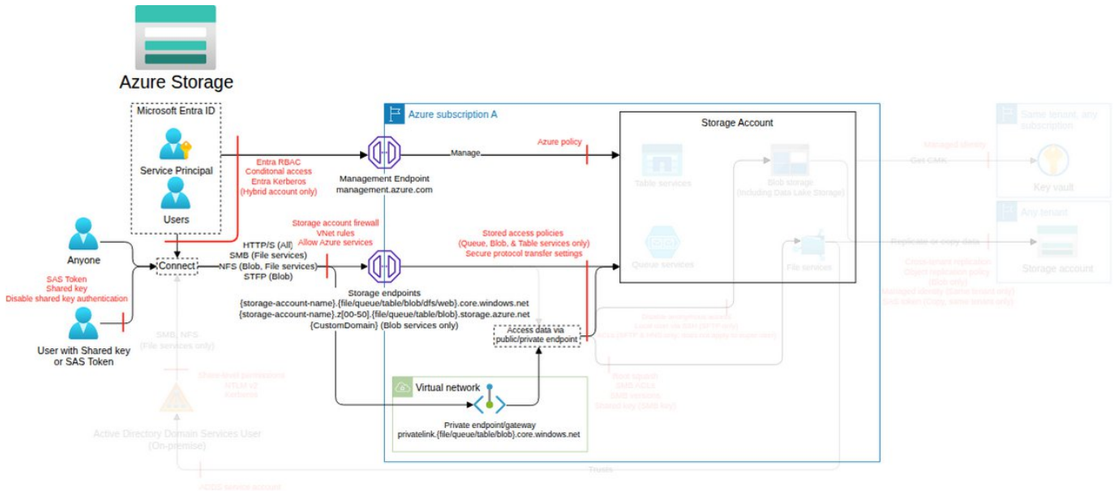
Threat Id	Storage.T25
Name	Delete data using Blob Storage lifecycle management
Description	Blob Storage lifecycle management allows implementing rule-based policies that automatically transition data to cooler tiers or expire it when it's no longer needed. An attacker can create or modify the Blob Storage lifecycle management settings to delete data or impact data latency.
Goal	Data manipulation
MITRE ATT&CK®	TA0040
CVSS	Medium (5.2)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/managementPolicies/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C15 - Maintain a list of the blob storage containers that are required to have a minimum retention period enabled. C17 - Prevent the creation of required storage accounts without the blob soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/deleteRetentionPolicy.enabled": false} in Deny mode). C19 - Ensure required storage accounts have the soft-delete option enabled for the containers. C20 - Prevent the creation of containers without the soft-delete option enabled (e.g., by using a custom Azure Policy on "Microsoft.Storage/storageAccounts/blobServices/containers/softDelete" in Deny mode).	High	2	2	-

Service compromise by disabling soft delete

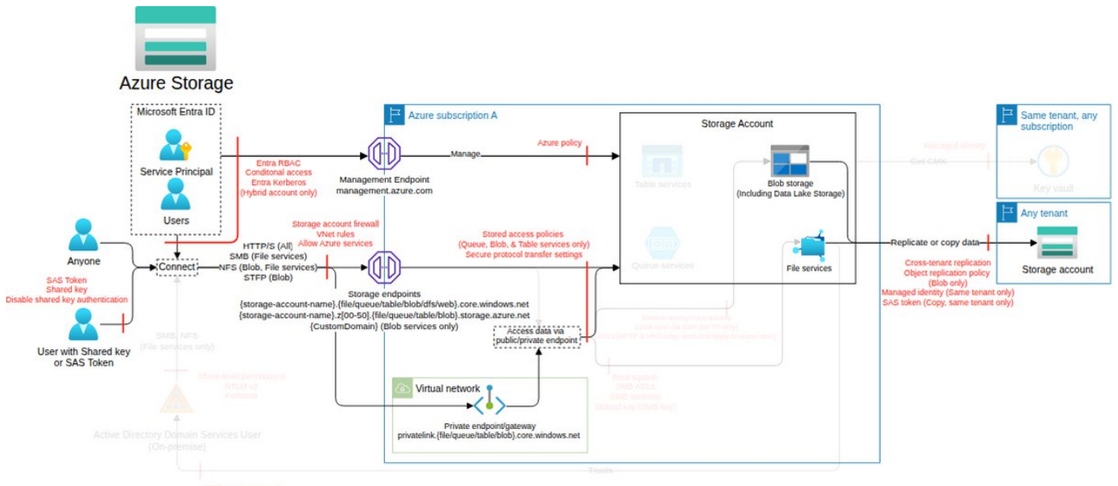
Threat Id	Storage.T39
Name	Service compromise by disabling soft delete
Description	Disabling blob soft delete allows the ability to continue recovering soft-deleted objects in the storage account until the soft delete retention period has elapsed. An attacker can disable soft delete to compromise the service.
Goal	Launch another attack
MITRE ATT&CK®	TA0004
CVSS	Medium (5.2)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C15 - Maintain a list of the blob storage containers that are required to have a minimum retention period enabled. C17 - Prevent the creation of required storage accounts without the blob soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/deleteRetentionPolicy.enabled": false} in Deny mode). C19 - Ensure required storage accounts have the soft-delete option enabled for the containers. C20 - Prevent the creation of containers without the soft-delete option enabled (e.g., by using a custom Azure Policy on "Microsoft.Storage/storageAccounts/blobServices/containers/softDelete" in Deny mode).	High	2	2	-

Denial of Service by removing replication

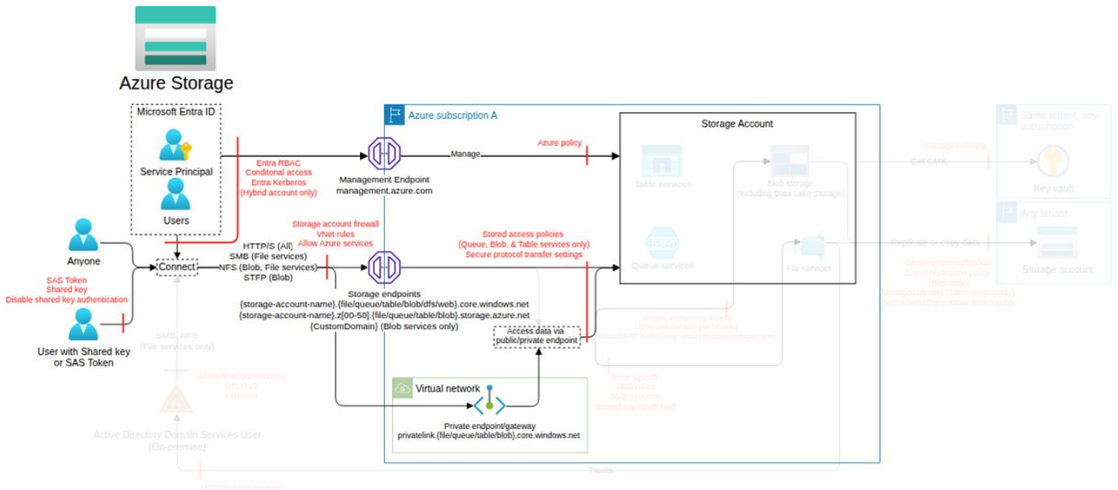
Threat Id	Storage.T42
Name	Denial of Service by removing replication
Description	Replication is a level of integrity protection and backup. An attacker can remove replication to affect data protection in the event of a fail over.
Goal	Data manipulation
MITRE ATT&CK®	TA0040
CVSS	Medium (5.2)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C47 - Maintain a list of storage accounts that require cross-tenant replication and their allowed destination tenants. C48 - Ensure only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized.	Very High	2	-	-
CO11 - Enable enhanced monitoring and notifications for storage accounts C50 - Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations. C51 - Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Low	2	-	-

Unauthorized access to data via storage account replication

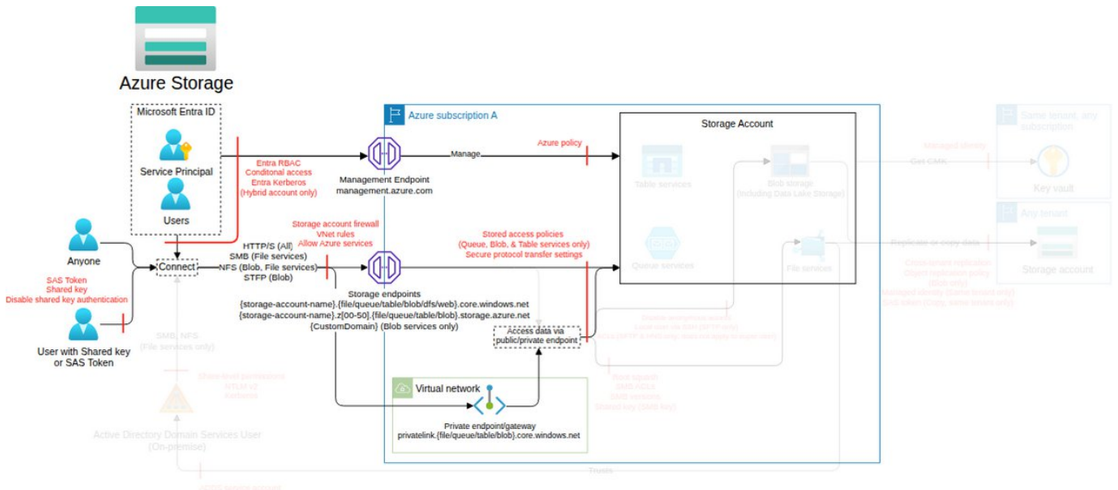
Threat Id	Storage.T13
Name	Unauthorized access to data via storage account replication
Description	Replication allows you to replicate objects and their metadata. An attacker can configure replication on a storage account to replicate objects (or their metadata or tags) to exfiltrate data.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Medium (5.2)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C47 - Maintain a list of storage accounts that require cross-tenant replication and their allowed destination tenants. C48 - Ensure only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized. C147 - Maintain a list of storage blobs that require Azure Backup. C150 - Maintain a list of authorized replication policies and their destination storage accounts. C151 - Ensure replication policies and their destination storage accounts are authorized.	Very High	5	-	-
CO11 - Enable enhanced monitoring and notifications for storage accounts C50 - Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations. C51 - Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Low	2	-	-

DoS due to storage account access key regeneration

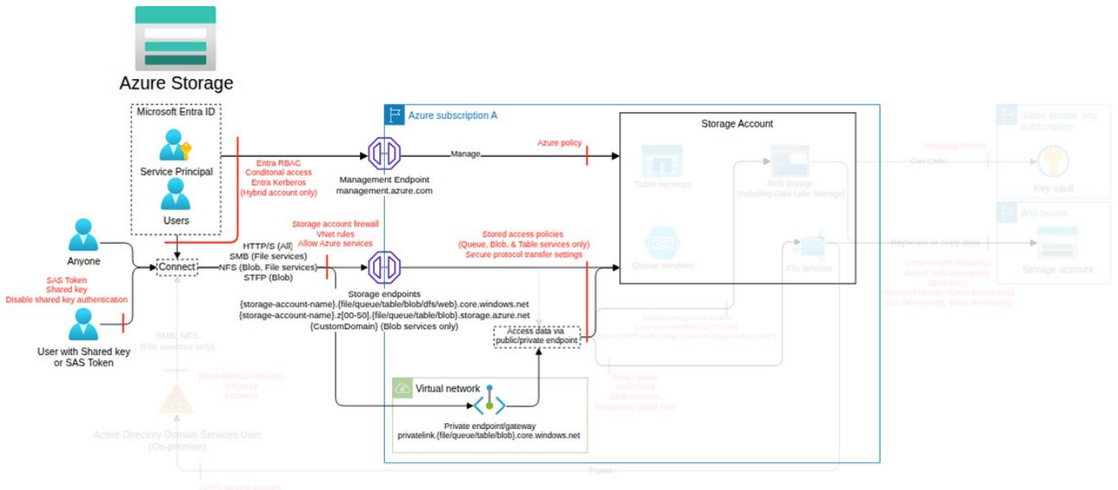
Threat Id	Storage.T2
Name	DoS due to storage account access key regeneration
Description	SAS tokens can be signed from a storage account access key, enabling non-Azure applications to access data in a storage account. An attacker can rotate or regenerate a storage account access key to invalidate its SAS tokens, blocking data access to any applications using SAS tokens derived from this access key.
Goal	Disruption of Service
MITRE ATT&CK®	TA0040
CVSS	Medium (4.5)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/regenerateKey/action", "Microsoft.Storage/storageAccounts/rotateKey/action"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-

Unauthorized data exposure by modifying CORS settings

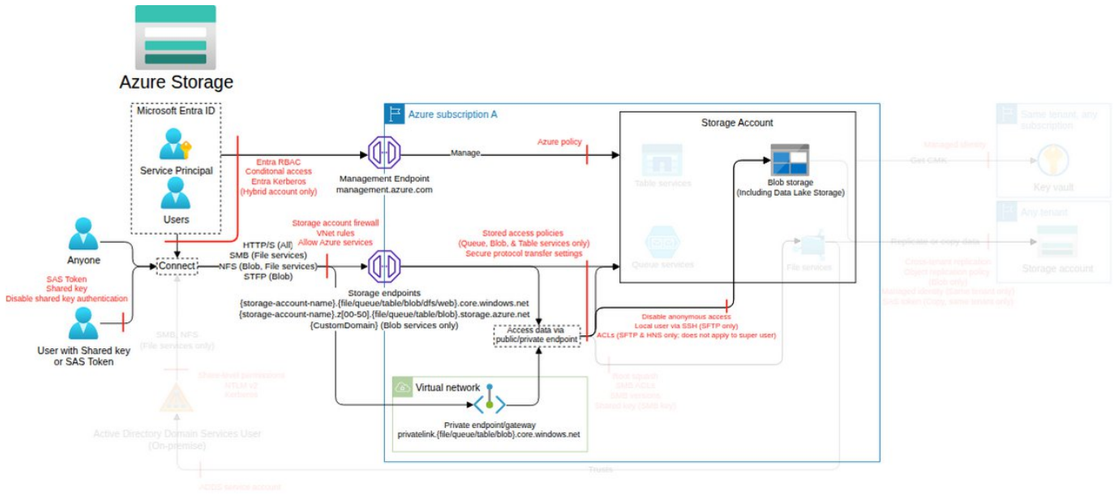
Threat Id	Storage.T26
Name	Unauthorized data exposure by modifying CORS settings
Description	CORS is an HTTP feature that enables a web application running under one domain to access resources in another domain. An attacker can modify the CORS policy on a storage account if it has HTTP access enabled and gain privileged access via origin reflection, enticing a user to access a page with a malicious script and return sensitive data.
Goal	Launch another attack
MITRE ATT&CK®	TA0004
CVSS	Medium (4.0)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO14 - Restrict and manage external websites (origins) that can make browser-based requests to storage accounts C94 - Maintain a list of authorized CORS per endpoint, trusted origins, and corresponding settings. C95 - Ensure only authorized storage accounts have CORS-trusted origins and corresponding settings configured. C96 - Prevent unauthorized storage accounts from using CORS trusted origins and corresponding settings (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/cors.allowedOrigins[*]": ["https://myapp.contoso.com"]} in Deny mode).	High	2	1	-

Unauthorized failover through configuration change

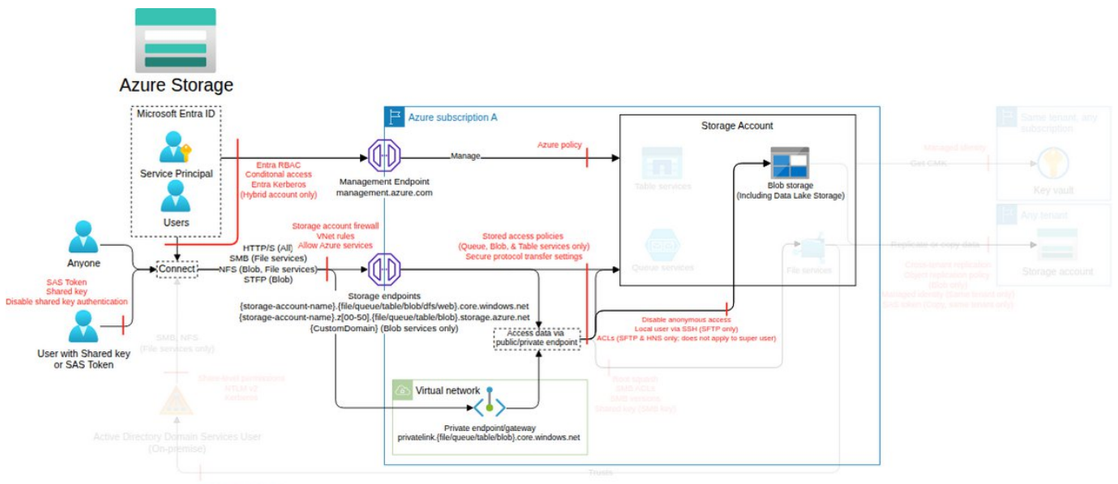
Threat Id	Storage.T59
Name	Unauthorized failover through configuration change
Description	Azure Storage accounts support failover, which transitions geo-redundant storage accounts from their primary region to the secondary, deleting the original primary data and converting the account to locally redundant storage. An attacker can initiate an unauthorized failover to disrupt availability, cause loss of unreplicated data, degrade redundancy, and introduce inconsistencies due to asynchronous replication.
Goal	Disruption of Service
MITRE ATT&CK®	TA0040
CVSS	Low (3.5)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/failover/action" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C75 - Maintain a list of authorized storage account regions that can be used for redundancy. C76 - Ensure the authorized storage account region used for redundancy is configured. C77 - Ensure only the authorized storage account region is set for redundancy (e.g., by using a custom Azure Policy on {"location": ["eastus","westeurope"]} in Deny mode).	High	2	1	-

Information disclosure due to unencrypted blob storage

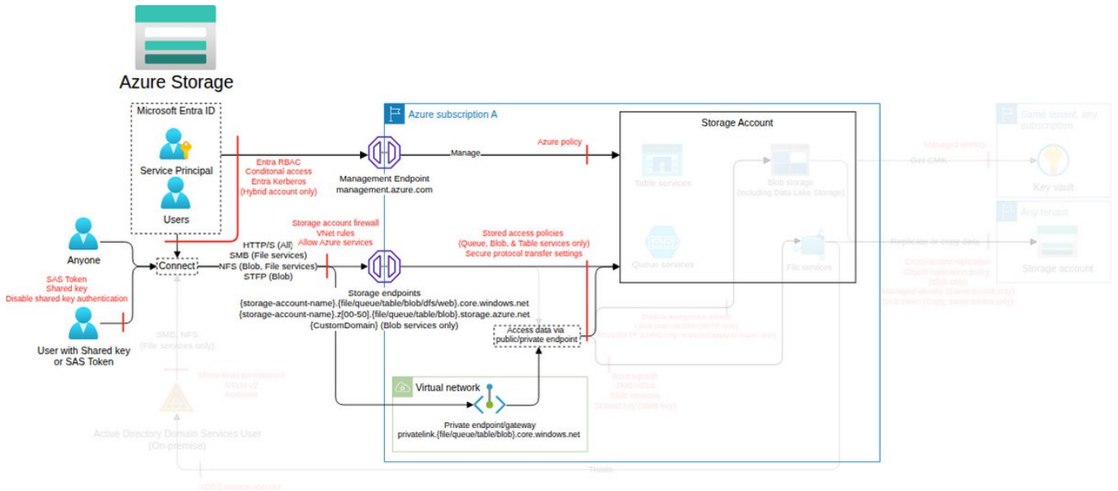
Threat Id	Storage.T49
Name	Information disclosure due to unencrypted blob storage
Description	A blob created before October 20, 2017 may not have been encrypted and must be recreated to enforce encryption. An attacker can abuse this to gain access to sensitive data.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Low (3.5)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/read" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-

Access to Storage account resources by modifying virtual network rules

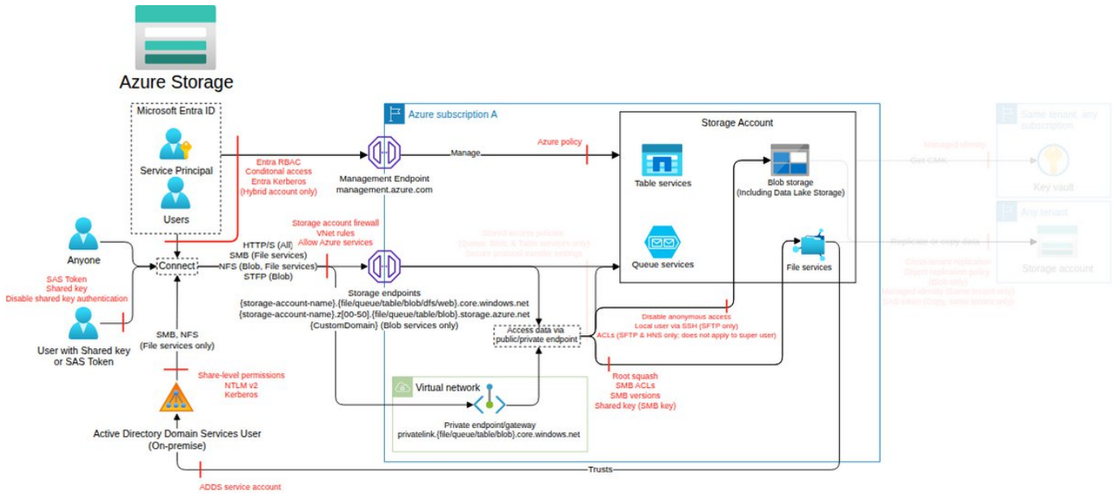
Threat Id	Storage.T50
Name	Access to Storage account resources by modifying virtual network rules
Description	Administrators configure network rules to allow only requests originating from authorized subnets. An attacker can insert or modify the rules to gain access.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Low (3.4)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts. C42 - Maintain a list of authorized IPs that are permitted through each storage account firewall. C43 - Ensure each storage account firewall only allows authorized IPs. C44 - Prevent access from unauthorized IPs by allowing only authorized IPs through the Azure Storage firewall (by using built-in Azure Policy "Storage accounts should restrict network access" in Deny mode).	Very High	4	1	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C6 - Maintain a list of storage accounts that require public access to be enabled. C7 - Ensure only required storage accounts have public access enabled. C8 - Prevent the creation or update of non-required storage accounts with public access enabled (e.g., by using Azure built-in policy "Storage accounts should disable public network access" in Deny mode). C55 - Maintain a list of blobs and containers that require anonymous access. C56 - Ensure anonymous access is set only for required blobs and containers. C57 - Ensure only required blobs and containers are anonymously accessible (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/containers/publicAccess": "Blob"} in Deny mode).	Medium	4	2	-

Defense evasion by modifying diagnostic settings

Threat Id	Storage.T10
Name	Defense evasion by modifying diagnostic settings
Description	An attacker can alter diagnostic settings at the storage account or container level, allowing them to redirect storage account logs to another tenant or subscription to exfiltrate data.
Goal	Launch another attack
MITRE ATT&CK®	TA0005
CVSS	Low (2.4)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/services/diagnosticsettings/write", "Microsoft.Storage/storageAccounts/providers/Microsoft.Insights/diagnosticsettings/write", "Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/diagnosticsettings/write", "Microsoft.Storage/storageAccounts/tableServices/providers/Microsoft.Insights/diagnosticsettings/write", "Microsoft.Storage/storageAccounts/fileServices/providers/Microsoft.Insights/diagnosticsettings/write", "Microsoft.Storage/storageAccounts/queueServices/providers/Microsoft.Insights/diagnosticsettings/write"] }

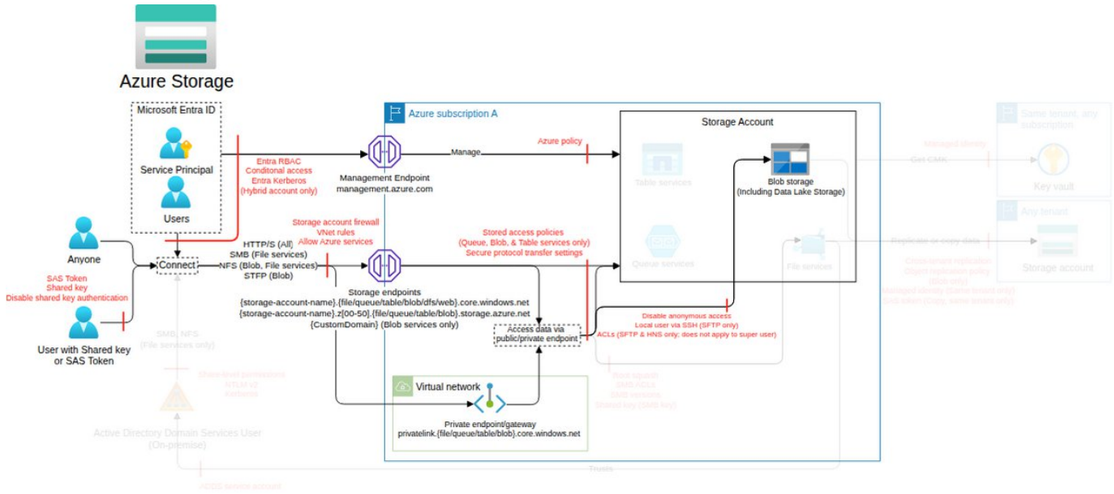


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO11 - Enable enhanced monitoring and notifications for storage accounts C50 - Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations. C51 - Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Low	2	-	-
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very Low	1	-	-

Blob storage *(subclass of Storage account, FC2)*

Object storage solution for storing unstructured data (blobs) accessible via HTTP/S and optionally via the Network File System (NFS) v3 and SFTP protocols.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

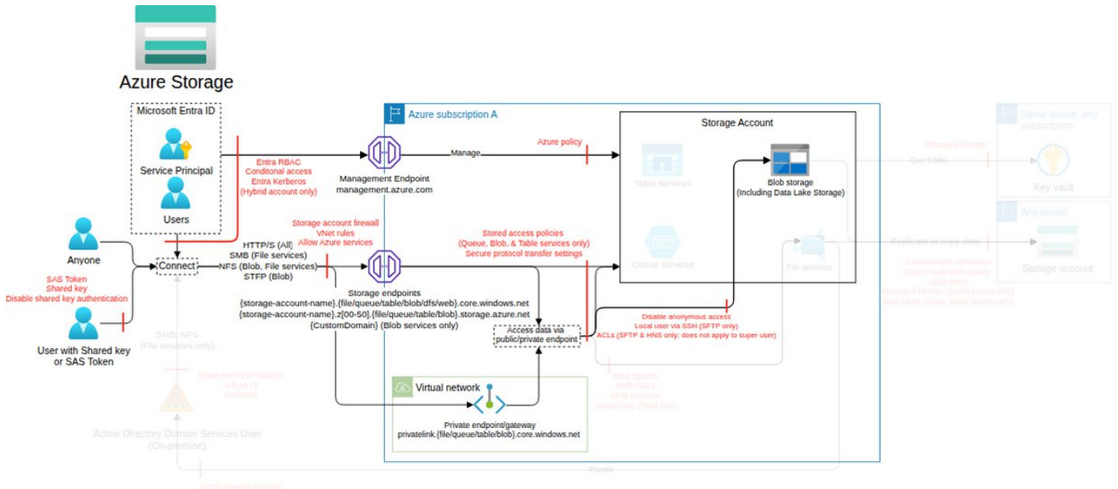
Action	IAM Permission
Creates a new container under the specified account. If the container with the same name already exists, the operation fails returns all user-defined metadata and system properties for the specified container. The data returned does not include the container's list of blobs operation marks the specified container for deletion. The container and any blobs contained within it are later deleted during garbage collection restype.	Microsoft.Storage/storageAccounts/blobServices/containers/write

Threat List

Name	CVSS
Unauthorized access to data by allowing anonymous public access	High (8.1)
Privilege escalation through modification of ACL	High (8.1)
Encrypt/overwrite files with ransomware in DFS/blob	Medium (6.1)
Unauthorized modification of data	Medium (5.7)
Recursively delete DFS directories and their content	Medium (5.2)
Execution of malware through file replacement	Medium (5.1)
Cost increase by executing Azure Data Lake Storage query acceleration	Medium (4.6)
Exfiltrate files via the static website feature	Medium (4.6)

Unauthorized access to data by allowing anonymous public access

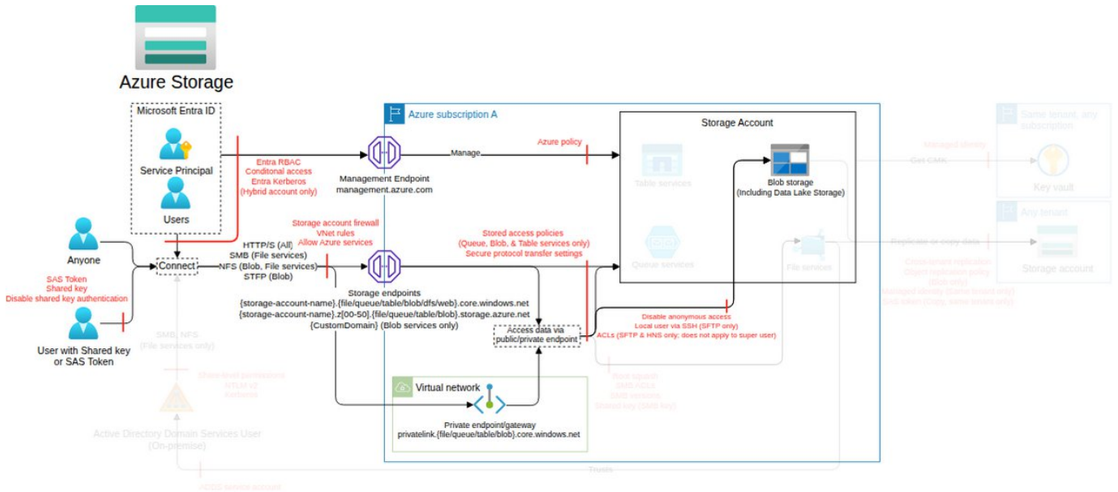
Threat Id	Storage.T5
Name	Unauthorized access to data by allowing anonymous public access
Description	Azure Storage account blobs support anonymous public access. An attacker can create or modify a container to make it public and steal/exfiltrate/expose data.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	High (8.1)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/blobServices/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts. C42 - Maintain a list of authorized IPs that are permitted through each storage account firewall. C43 - Ensure each storage account firewall only allows authorized IPs.	Very High	4	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C6 - Maintain a list of storage accounts that require public access to be enabled. C7 - Ensure only required storage accounts have public access enabled. C8 - Prevent the creation or update of non-required storage accounts with public access enabled (e.g., by using Azure built-in policy "Storage accounts should disable public network access" in Deny mode). C55 - Maintain a list of blobs and containers that require anonymous access. C56 - Ensure anonymous access is set only for required blobs and containers. C57 - Ensure only required blobs and containers are anonymously accessible (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/containers/publicAccess": "Blob"} in Deny mode).	High	5	2	-

Privilege escalation through modification of ACL

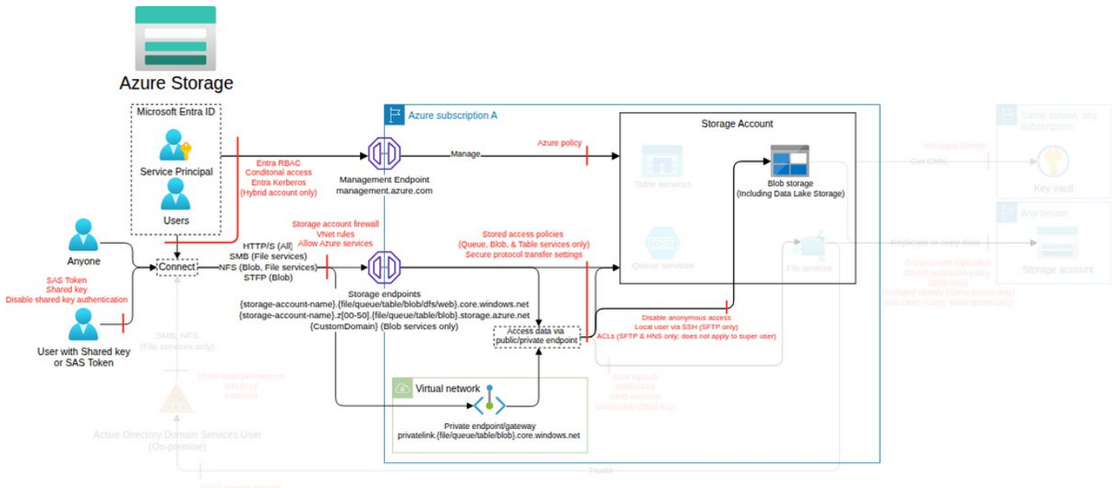
Threat Id	Storage.T66
Name	Privilege escalation through modification of ACL
Description	Azure Data Lake Storage containers support Access Control Lists (ACLs). An attacker can modify these ACLs to escalate their permissions.
Goal	Launch another attack
MITRE ATT&CK®	TA0004
CVSS	High (8.1)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/write"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO7 - Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model C158 - Maintain a list of authorized Access Control Lists (ACLs) on Data Lake Storage containers. C159 - Ensure all Access Control Lists (ACLs) on Data Lake Storage containers are authorized.	Medium	2	-	-

Encrypt/overwrite files with ransomware in DFS/blob

Threat Id	Storage.T9
Name	Encrypt/overwrite files with ransomware in DFS/blob
Description	An attacker can encrypt or overwrite files and objects in DFS or blobs using an encryption key under their control and request a ransom to access the decryption key.
Goal	Direct Financial Gain
MITRE ATT&CK®	TA0040
CVSS	Medium (6.1)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "directory:RWX;file:RWX"] }

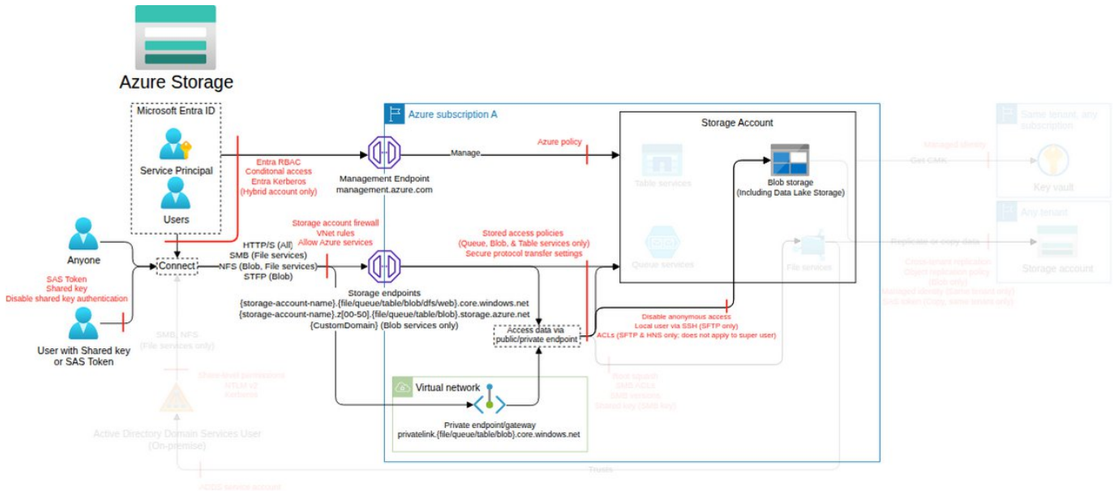


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C32 - Maintain a list of storage container blobs that require immutability and soft delete. C33 - Ensure required storage container blobs have immutability and soft delete enabled.	Very High	2	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C26 - Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed permissions. C27 - Ensure SAS token authentication is enabled only for storage accounts that allow it.	High	3	-	-
CO12 - Enforce encryption on data at rest and protect encryption keys C60 - Maintain a list of authorized customer-managed keys used by storage accounts. C61 - Ensure only authorized customer-managed keys are configured for storage accounts. C63 - Prevent storage accounts that require customer-managed keys from using service-managed keys (e.g., by using built-in Azure Policy "Storage accounts should use customer-managed key for encryption" in Deny mode).	High	2	1	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C15 - Maintain a list of the blob storage containers that are required to have a minimum retention period enabled. C16 - Ensure required storage accounts have the soft-delete feature for blobs enabled for the defined minimum retention period. C17 - Prevent the creation of required storage accounts without the blob soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/deleteRetentionPolicy.enabled": false} in Deny mode). C19 - Ensure required storage accounts have the soft-delete option enabled for the containers. C20 - Prevent the creation of containers without the soft-delete option enabled (e.g., by using a custom Azure Policy on "Microsoft.Storage/storageAccounts/blobServices/containers/softDelete" in Deny mode). C46 - Ensure storage blobs are using Azure Backup, following the requirements in the Azure Backup ThreatModel. C147 - Maintain a list of storage blobs that require Azure Backup. C150 - Maintain a list of authorized replication policies and their destination storage accounts.	High	6	2	-
CO11 - Enable enhanced monitoring and notifications for storage accounts C50 - Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations.	Low	2	-	-

C51 - Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.				

Unauthorized modification of data

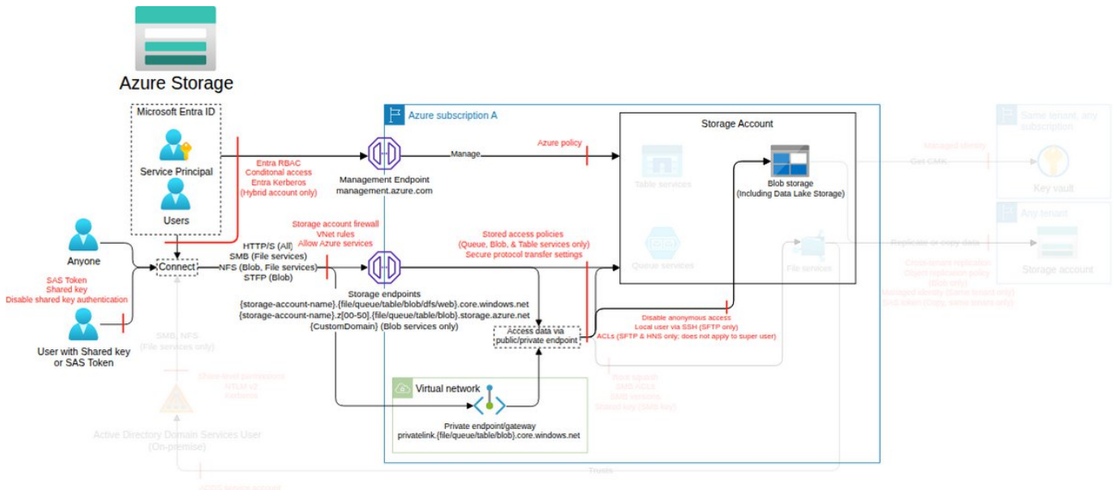
Threat Id	Storage.T8
Name	Unauthorized modification of data
Description	Blob storage in Azure allows CRUD operations. An attacker can modify data, leading to data manipulation.
Goal	Data manipulation
MITRE ATT&CK®	TA0040
CVSS	Medium (5.7)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C32 - Maintain a list of storage container blobs that require immutability and soft delete. C33 - Ensure required storage container blobs have immutability and soft delete enabled.	Very High	2	-	-
CO11 - Enable enhanced monitoring and notifications for storage accounts C50 - Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations. C51 - Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Low	2	-	-

Recursively delete DFS directories and their content

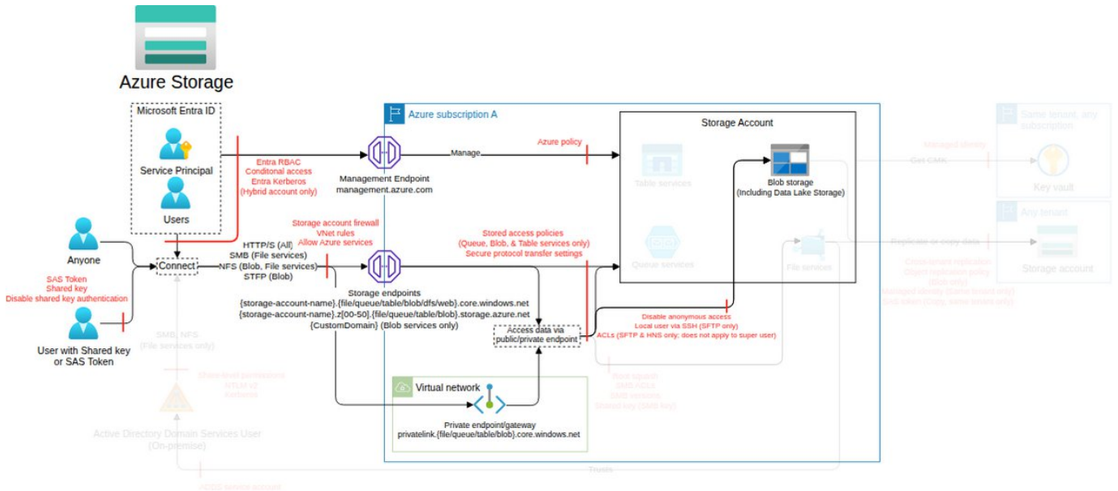
Threat Id	Storage.T7
Name	Recursively delete DFS directories and their content
Description	Distributed file systems have a hierarchical architecture. An attacker can delete multiple directories and files recursively to make them unavailable.
Goal	Disruption of Service
MITRE ATT&CK®	TA0040
CVSS	Medium (5.2)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete", "Microsoft.Storage/storageAccounts/blobServices/containers/delete"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C32 - Maintain a list of storage container blobs that require immutability and soft delete. C144 - Maintain a list of storage account blobs that require versioning and blob change feed to be enabled.	Very High	2	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C10 - Ensure versioning is enabled on required containers. C12 - Ensure snapshots are enabled for required file shares. C15 - Maintain a list of the blob storage containers that are required to have a minimum retention period enabled. C16 - Ensure required storage accounts have the soft-delete feature for blobs enabled for the defined minimum retention period. C19 - Ensure required storage accounts have the soft-delete option enabled for the containers. C46 - Ensure storage blobs are using Azure Backup, following the requirements in the Azure Backup ThreatModel. C145 - Maintain a list of Azure Files that require snapshots. C147 - Maintain a list of storage blobs that require Azure Backup. C150 - Maintain a list of authorized replication policies and their destination storage accounts.	High	9	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token).	High	1	-	-
CO21 - Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model C22 - Maintain a list of storage accounts that require hierarchical namespace (i.e., Data Lake Storage) and SSH enabled. C23 - Ensure all required storage accounts have hierarchical namespace (i.e., Data Lake Storage) enabled.	Medium	2	-	-
CO11 - Enable enhanced monitoring and notifications for storage accounts C50 - Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations. C51 - Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Low	2	-	-

Execution of malware through file replacement

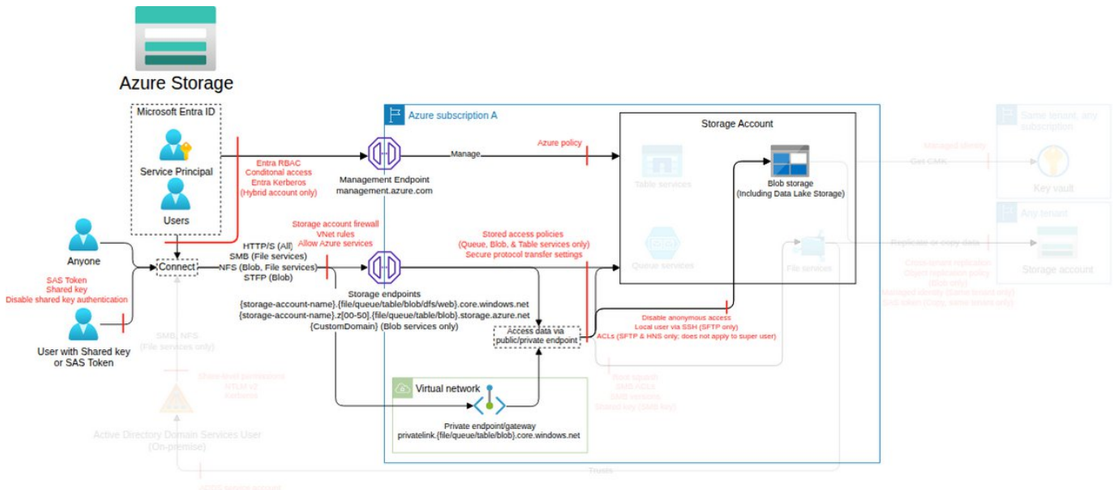
Threat Id	Storage.T12
Name	Execution of malware through file replacement
Description	Blob storage supports any file object. An attacker can overwrite a legitimate file with malware and infect internal services or external users.
Goal	Launch another attack
MITRE ATT&CK®	TA0003
CVSS	Medium (5.1)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C32 - Maintain a list of storage container blobs that require immutability and soft delete. C33 - Ensure required storage container blobs have immutability and soft delete enabled. C110 - Prevent modification or deletion of required storage accounts by using a resource lock set to read-only and/or delete, using the Azure Resource Manager ThreatModel.	Very High	2	1	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts. C42 - Maintain a list of authorized IPs that are permitted through each storage account firewall. C43 - Ensure each storage account firewall only allows authorized IPs.	Very High	4	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C26 - Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed permissions. C27 - Ensure SAS token authentication is enabled only for storage accounts that allow it.	High	3	-	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C15 - Maintain a list of the blob storage containers that are required to have a minimum retention period enabled. C16 - Ensure required storage accounts have the soft-delete feature for blobs enabled for the defined minimum retention period. C19 - Ensure required storage accounts have the soft-delete option enabled for the containers. C46 - Ensure storage blobs are using Azure Backup, following the requirements in the Azure Backup ThreatModel. C147 - Maintain a list of storage blobs that require Azure Backup. C150 - Maintain a list of authorized replication policies and their destination storage accounts.	High	6	-	-

Cost increase by executing Azure Data Lake Storage query acceleration

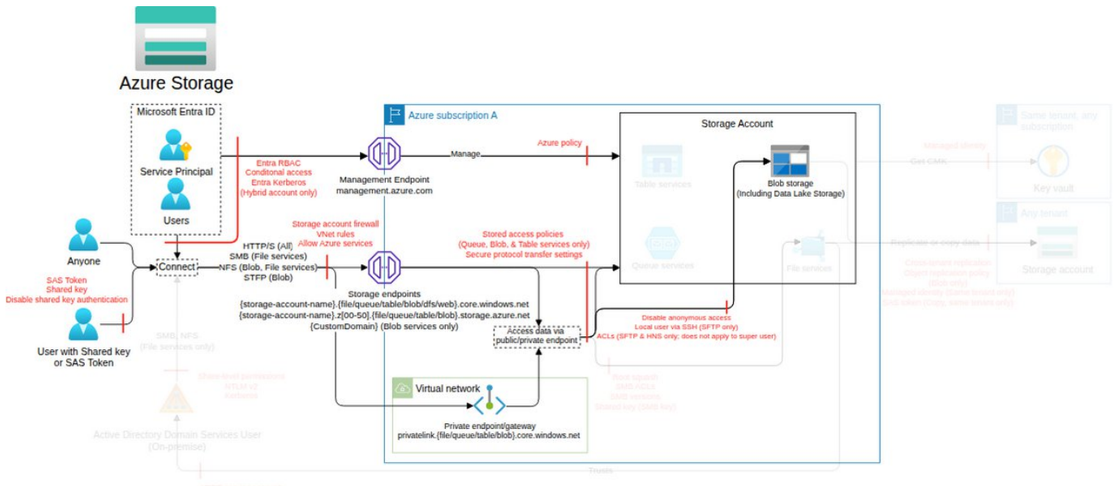
Threat Id	Storage.T34
Name	Cost increase by executing Azure Data Lake Storage query acceleration
Description	Query acceleration is used for data processing applications and can be executed on a storage account. Due to the increased compute load within the Azure Data Lake Storage service, the pricing model for query acceleration differs from the normal Azure Data Lake Storage transaction model. An attacker can execute the queries and generate costs.
Goal	Financial Drain
MITRE ATT&CK®	TA0040
CVSS	Medium (4.6)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token).	High	1	-	-

Exfiltrate files via the static website feature

Threat Id	Storage.T22
Name	Exfiltrate files via the static website feature
Description	A storage account can be configured as a static website server. An attacker can distribute malicious and infected files or exfiltrate data via a website hosted on a storage account (i.e., through the $web directory).
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Medium (4.6)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write" }

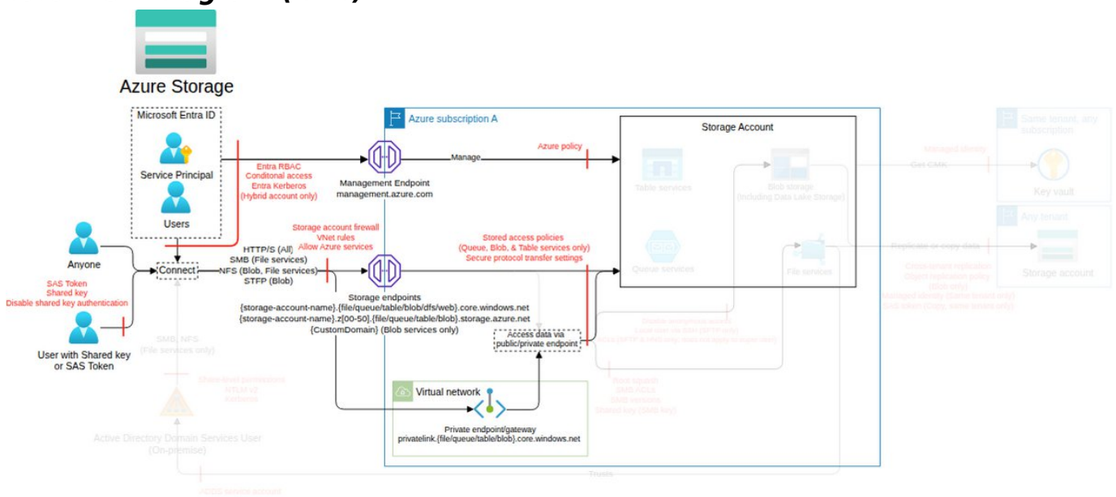


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C90 - Maintain a list of storage accounts that require static website hosting. C91 - Ensure only storage accounts that require static website hosting have it enabled. C92 - Prevent storage accounts that do not require static website hosting from having it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/staticWebsite.enabled": true} in Deny mode).	Medium	2	1	-

Blob inventory *(subclass of Blob storage, FC10)*

The Azure Storage blob inventory feature provides an overview of your containers, blobs, snapshots, and blob versions within a storage account. Use the inventory report to understand various attributes of blobs and containers, such as the total data size, age, encryption status, immutability policy, and legal hold.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

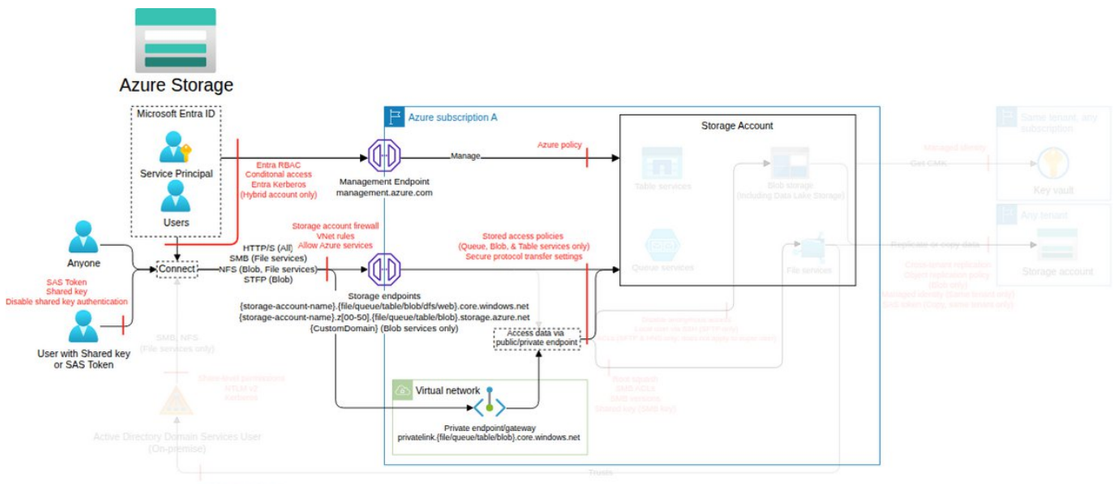
Action	IAM Permission
Sets the blob inventory policy to the specified storage account.	Microsoft.Storage/storageAccounts/inventoryPolicies/write

Threat List

Name	CVSS
Exfiltrate metadata using blob inventory functionality	Low (3.5)

Exfiltrate metadata using blob inventory functionality

Threat Id	Storage.T24
Name	Exfiltrate metadata using blob inventory functionality
Description	Storage blobs have inventory lists to track the objects they contain. An attacker can access the blob inventory, obtaining knowledge about running services, and exfiltrate metadata.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Low (3.5)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/inventoryPolicies/read", "Microsoft.Storage/storageAccounts/inventoryPolicies/write"] }

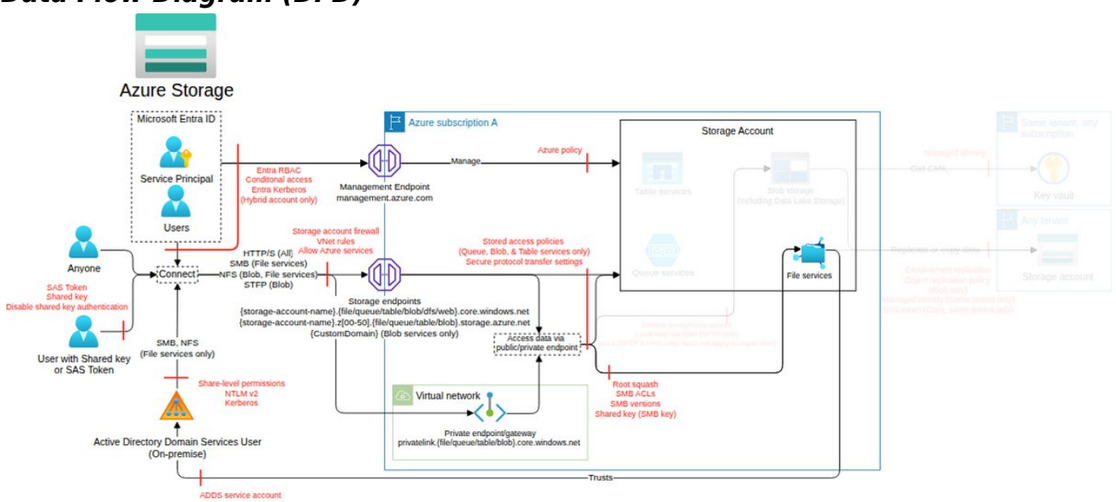


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-

File shares *(subclass of Storage account, FC3)*

Azure Files offers fully governed file shares in the cloud accessible via Server Message Block (SMB) protocol, Network File System (NFS) v4.1 protocol, or the in-preview Azure Files REST API.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

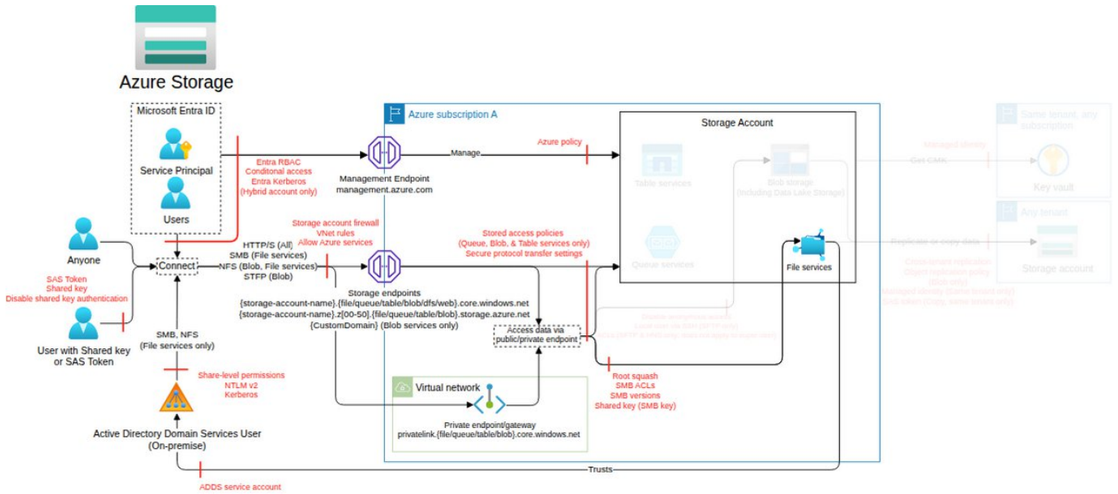
Action	IAM Permission
Creates a new share under the specified account as described by request body. The share resource includes metadata and properties for that share. It does not include a list of the files contained by the share. Updates share properties as specified in request body. Properties not mentioned in the request will not be changed. Update fails if the specified share does not already exist.	Microsoft.Storage/storageAccounts/fileServices/shares/write

Threat List

Name	CVSS
Recursively delete directories and their contents in the file share	Medium (6.1)
Distribute malicious files via file share	Medium (5.6)
Data exposure through exploitation of legacy protocols	Medium (4.2)
Exfiltrate data using different access methods	Low (3.7)
Denial of Wallet (DoW) through the upload of files to a storage account	Low (3.5)
Data exposure by changing encryption type	Low (2.4)

Recursively delete directories and their contents in the file share

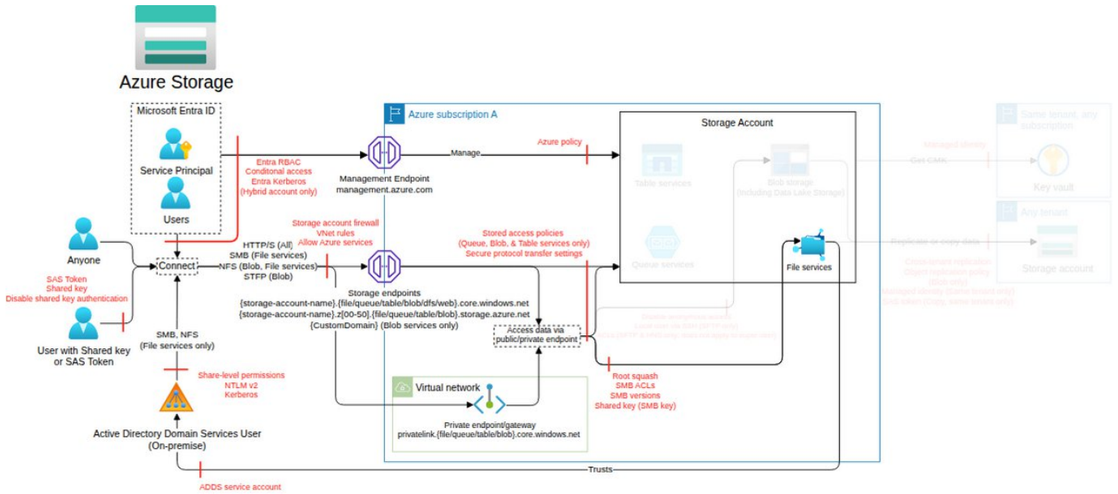
Threat Id	Storage.T18
Name	Recursively delete directories and their contents in the file share
Description	File shares, similar to the DFS, have a hierarchical architecture. An attacker can potentially delete multiple directories and files recursively.
Goal	Disruption of Service
MITRE ATT&CK®	TA0040
CVSS	Medium (6.1)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/delete" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO24 - Protect the integrity of blob storage data from unauthorized changes C107 - Maintain the list of storage accounts that should require read-only and/or delete locks. C108 - Ensure only required storage accounts have read-only and/or delete locks applied. C110 - Prevent modification or deletion of required storage accounts by using a resource lock set to read-only and/or delete, using the Azure Resource Manager ThreatModel.	Very High	2	1	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C83 - Define the minimum retention period for required file shares (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/deleteRetentionPolicy.days": 7} in Deny mode). C84 - Ensure file shares have the soft-delete option enabled for at least the defined minimum retention period. C85 - Prevent the creation of file shares without the soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/shares/deleteRetentionPolicy.enabled": false} in Deny mode).	Medium	2	1	-

Distribute malicious files via file share

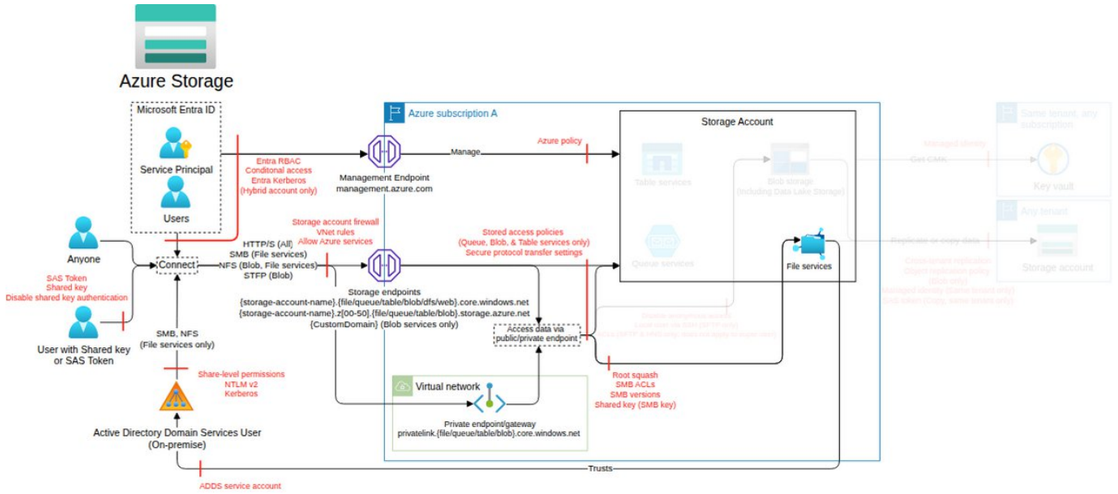
Threat Id	Storage.T20
Name	Distribute malicious files via file share
Description	File share services in Azure allow machines to mount the share via SMB. An attacker can distribute malicious files by uploading them to the file share service.
Goal	Launch another attack
MITRE ATT&CK®	TA0003
CVSS	Medium (5.6)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C149 - Ensure required blobs, file shares, queues, tables, and DFS are using authorized authentication methods.	High	2	-	-
CO8 - Enforce encryption in transit C120 - Maintain a list of required file shares' security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only). C121 - Ensure required file shares' security protocol settings are set. C122 - Prevent security protocol settings from changing on required file shares (e.g., by using custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb": {"kerberosTicketEncryption":"AES256","channelEncryption":"Required"}} in Deny mode).	High	2	1	-

Data exposure through exploitation of legacy protocols

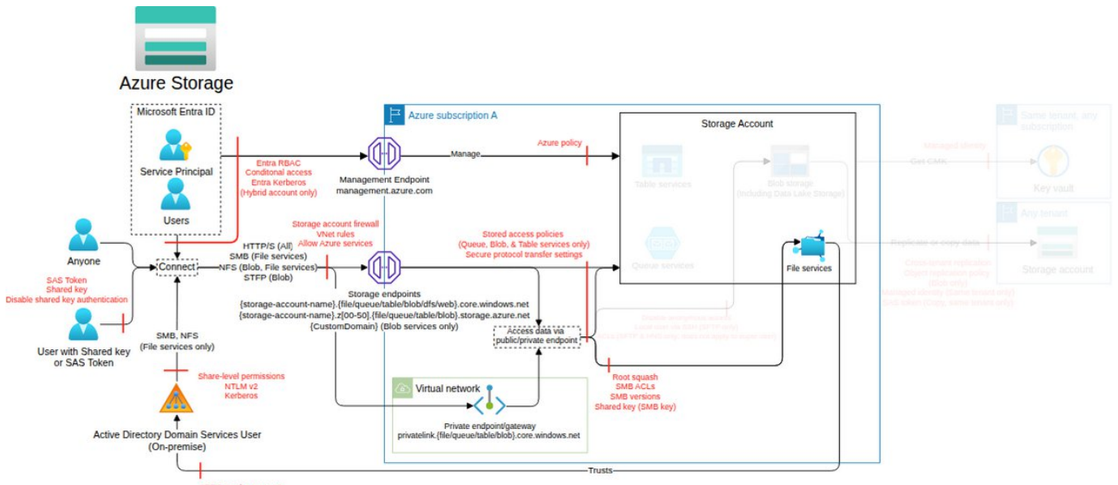
Threat Id	Storage.T61
Name	Data exposure through exploitation of legacy protocols
Description	Azure file shares support SMB version 2.1, which has several known vulnerabilities. An attacker can set the SMB version to a vulnerable one and abuse the protocol to collect sensitive data.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Medium (4.2)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO8 - Enforce encryption in transit C98 - Maintain a list of file shares that require NFS/SMB 2.1 enabled. C99 - Ensure only file shares that require NFS/SMB 2.1 have it enabled. C100 - Prevent file shares that do not require NFS/SMB 2.1 from being enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb.protocolVersions[*]": ["SMB2.1"]} in Deny mode). C101 - Monitor the creation or update of Azure Files NFS/SMB 2.1 and corresponding settings (e.g., using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly").	High	2	1	1

Exfiltrate data using different access methods

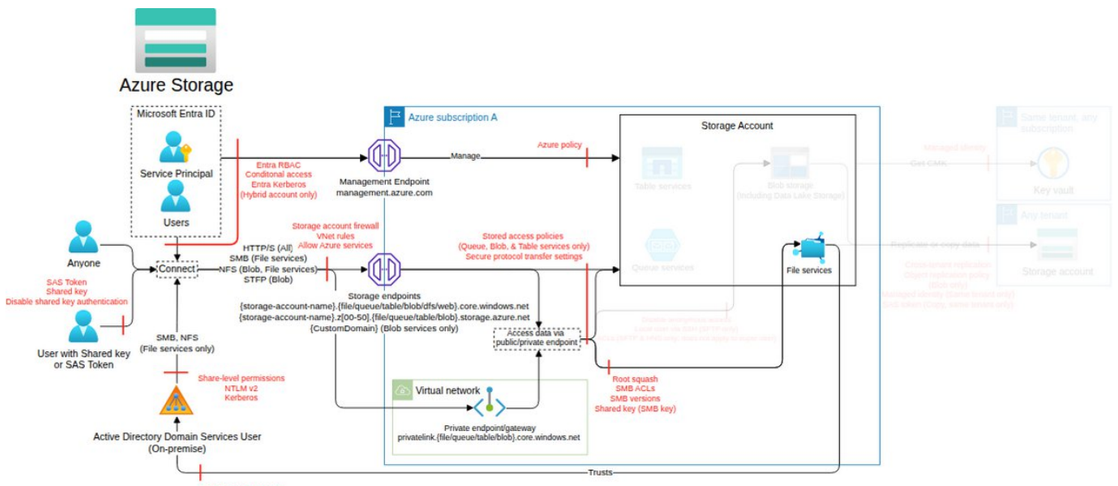
Threat Id	Storage.T15
Name	Exfiltrate data using different access methods
Description	Data stored on a file share using SMB or NFS v4.1 protocols can be accessed using REST APIs with the HTTP/S protocol. An attacker can access data using a different access method to gain access to the data.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Low (3.7)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/read" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts. C42 - Maintain a list of authorized IPs that are permitted through each storage account firewall. C43 - Ensure each storage account firewall only allows authorized IPs. C44 - Prevent access from unauthorized IPs by allowing only authorized IPs through the Azure Storage firewall (by using built-in Azure Policy "Storage accounts should restrict network access" in Deny mode).	Very High	4	1	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token).	High	1	-	-
CO8 - Enforce encryption in transit C120 - Maintain a list of required file shares' security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only). C121 - Ensure required file shares' security protocol settings are set.	High	2	-	-

Denial of Wallet (DoW) through the upload of files to a storage account

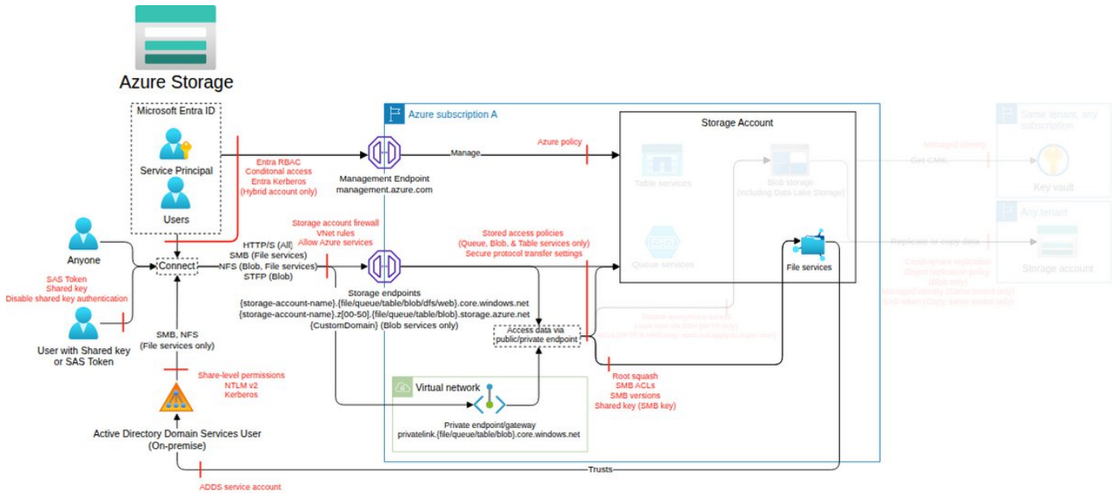
Threat Id	Storage.T16
Name	Denial of Wallet (DoW) through the upload of files to a storage account
Description	Blob storage is billed based on usage. An attacker can upload terabytes of data to the storage account and cause billing implications.
Goal	Financial Drain
MITRE ATT&CK®	TA0040
CVSS	Low (3.5)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-

Data exposure by changing encryption type

Threat Id	Storage.T60
Name	Data exposure by changing encryption type
Description	Azure file shares support different levels of encryption for data-in-transit, including no encryption. An attacker can disable encryption on a file share to expose the contents of the share.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Low (2.4)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write" }

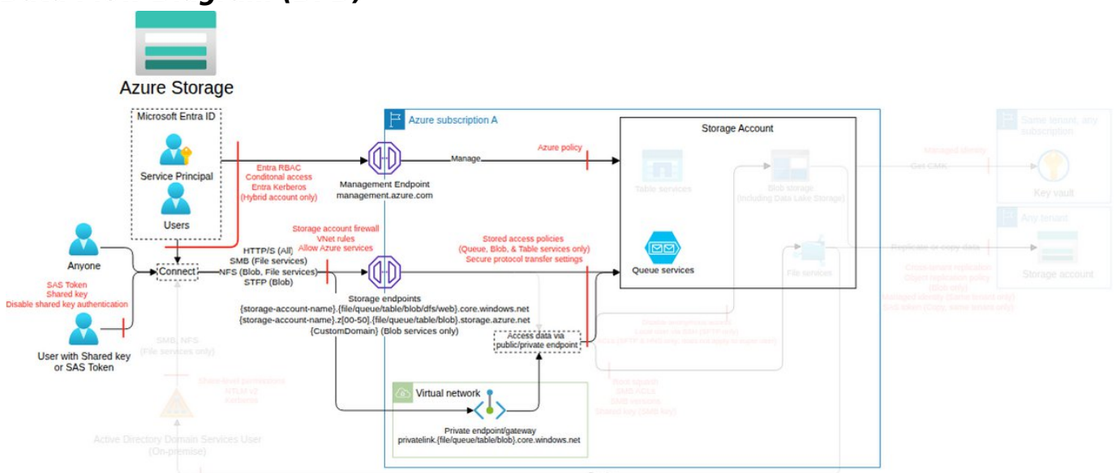


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO8 - Enforce encryption in transit C120 - Maintain a list of required file shares' security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only). C121 - Ensure required file shares' security protocol settings are set. C122 - Prevent security protocol settings from changing on required file shares (e.g., by using custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb": {"kerberosTicketEncryption":"AES256","channelEncryption":"Required"}} in Deny mode).	High	2	1	-
CO5 - Ensure backup, replication, and recovery capabilities for storage account services C71 - Maintain a list of storage accounts that require redundancy. C72 - Ensure required storage accounts use redundancy.	Low	2	-	-

Queues *(subclass of Storage account, FC4)*

Azure Queue Storage is a service for storing messages. Access messages via HTTP/S calls.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

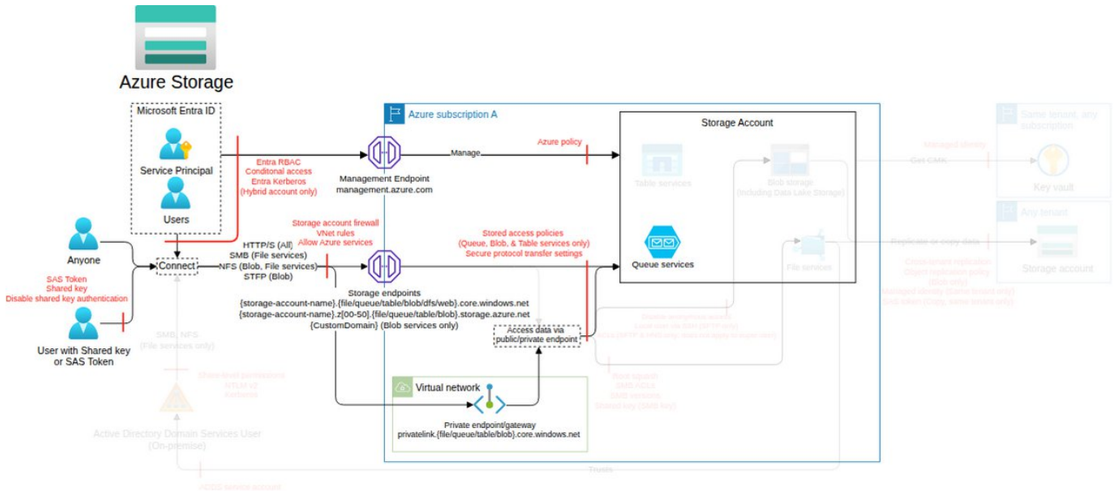
Action	IAM Permission
Creates a new queue with the specified queue name, under the specified account. Creates a new queue with the specified queue name, under the specified account.	Microsoft.Storage/storageAccounts/queueServices/queues/write

Threat List

Name	CVSS
Privilege escalation by modifying queue access policy	Medium (6.2)
Impacting queue's message integrity or complete loss of sensitive data	Medium (6.1)

Privilege escalation by modifying queue access policy

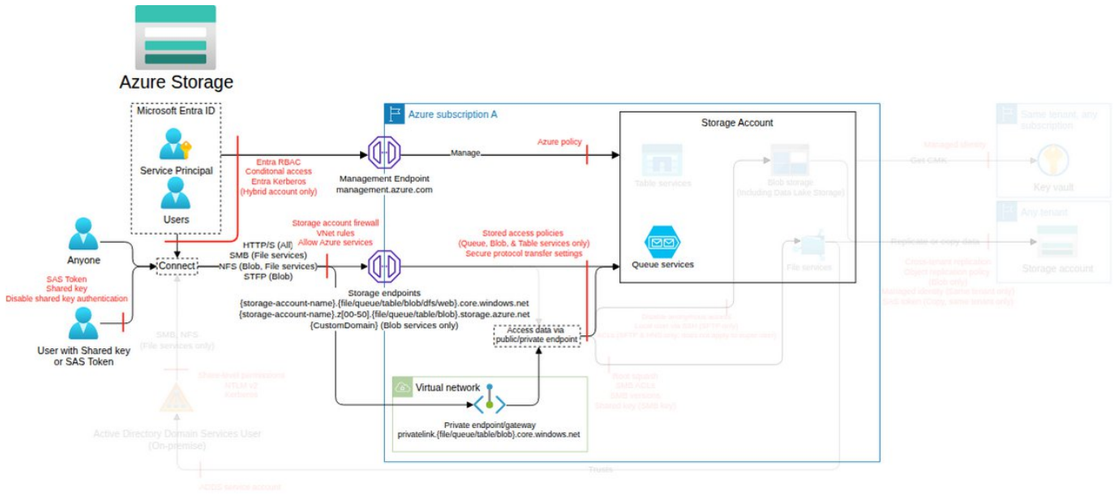
Threat Id	Storage.T27
Name	Privilege escalation by modifying queue access policy
Description	Queue access policies limit access to entities via the queue share endpoint when using a SAS token. An attacker can modify these access policies to escalate their privileges.
Goal	Launch another attack
MITRE ATT&CK®	TA0004
CVSS	Medium (6.2)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/queueServices/write", "Microsoft.Storage/storageAccounts/queueServices/queues/write"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C26 - Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed permissions. C156 - Ensure all stored access policy permissions are authorized on each container, file share, queue, and table.	High	3	-	-

Impacting queue's message integrity or complete loss of sensitive data

Threat Id	Storage.T31
Name	Impacting queue's message integrity or complete loss of sensitive data
Description	Messages in queues can be purged and deleted; queues can be deleted with all the messages, and queue parameter changes can result in losing all the messages. An attacker can delete or alter the messages and queues using any method, impacting downstream applications and processes, and causing loss of integrity and DoS.
Goal	Data manipulation
MITRE ATT&CK®	TA0040
CVSS	Medium (6.1)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/queueServices/write", "Microsoft.Storage/storageAccounts/queueServices/queues/write", "Microsoft.Storage/storageAccounts/queueServices/queues/delete"] }

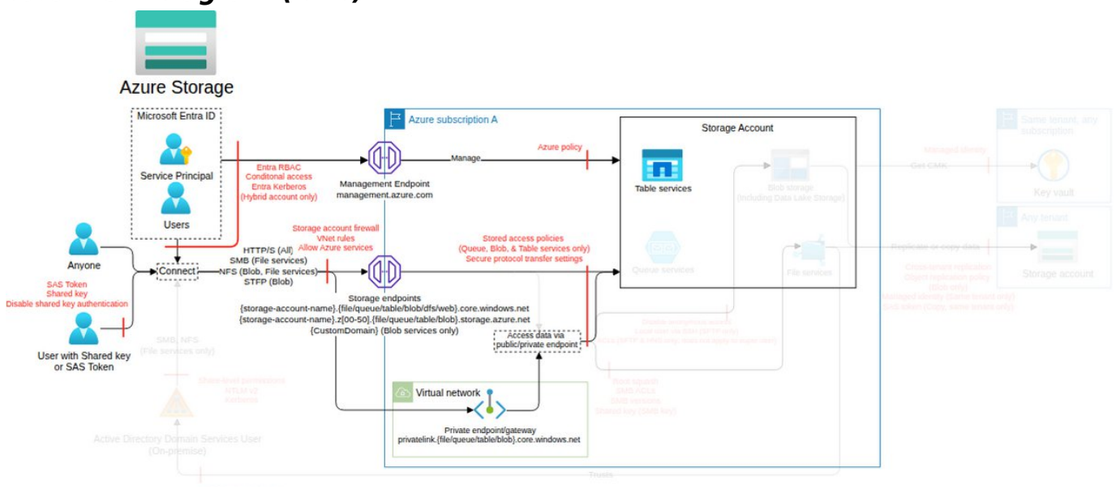


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts. C42 - Maintain a list of authorized IPs that are permitted through each storage account firewall. C43 - Ensure each storage account firewall only allows authorized IPs. C44 - Prevent access from unauthorized IPs by allowing only authorized IPs through the Azure Storage firewall (by using built-in Azure Policy "Storage accounts should restrict network access" in Deny mode).	Very High	4	1	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C26 - Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed permissions. C27 - Ensure SAS token authentication is enabled only for storage accounts that allow it.	High	3	-	-

Tables *(subclass of Storage account, FC5)*

Azure table storage is a service that stores non-relational structured data (or structured NoSQL data) in the cloud, providing a key/attribute store with a schemaless design.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

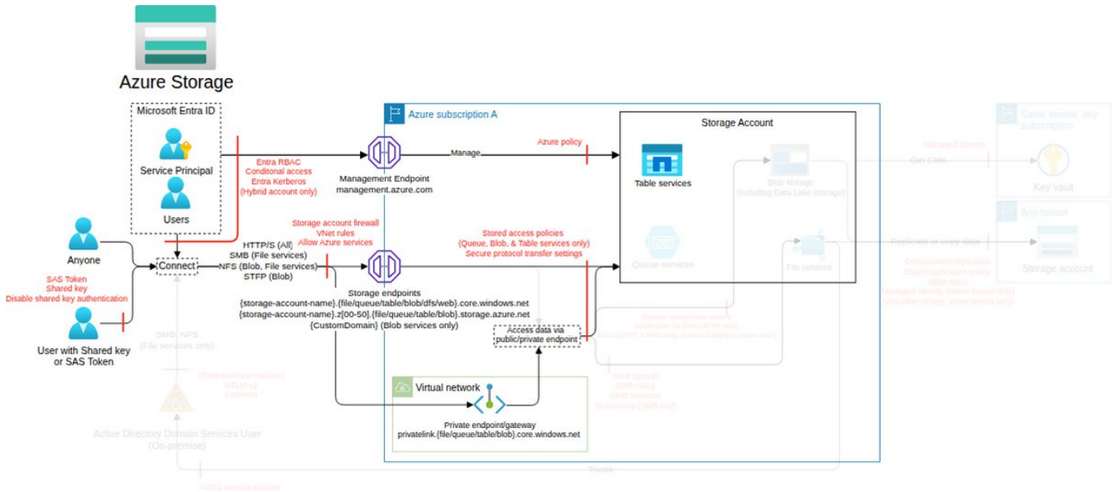
Action	IAM Permission
Creates a new table with the specified table name, under the specified account. Creates a new table with the specified table name, under the specified account.	Microsoft.Storage/storageAccounts/tableServices/tables/write

Threat List

Name	CVSS
Privilege escalation by modifying table access policy	Medium (6.2)

Privilege escalation by modifying table access policy

Threat Id	Storage.T28
Name	Privilege escalation by modifying table access policy
Description	Table access policies are used to limit access to entities via the table endpoint when using a SAS token. An attacker can modify these access policies to escalate their privileges.
Goal	Launch another attack
MITRE ATT&CK®	TA0004
CVSS	Medium (6.2)
IAM Access	{ "OR": ["Microsoft.Storage/storageAccounts/tableServices/write", "Microsoft.Storage/storageAccounts/tableServices/tables/write"] }

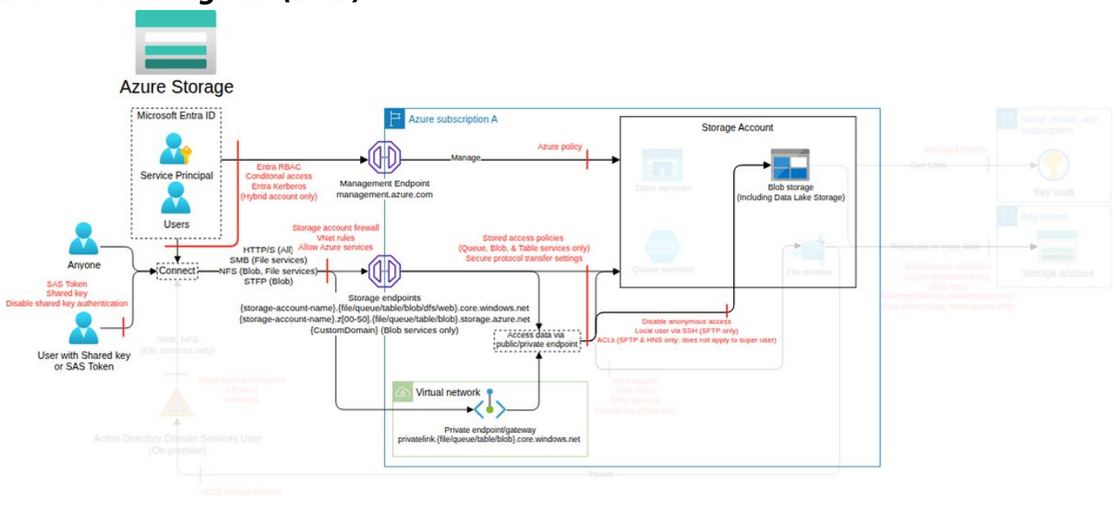


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C26 - Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed permissions. C156 - Ensure all stored access policy permissions are authorized on each container, file share, queue, and table.	High	3	-	-

Local users *(subclass of Storage account, FC11)*

Blob storage supports the SSH File Transfer Protocol (SFTP). This support lets you securely connect to blob storage via an SFTP endpoint, allowing you to use SFTP for file access, file transfer, and file management.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

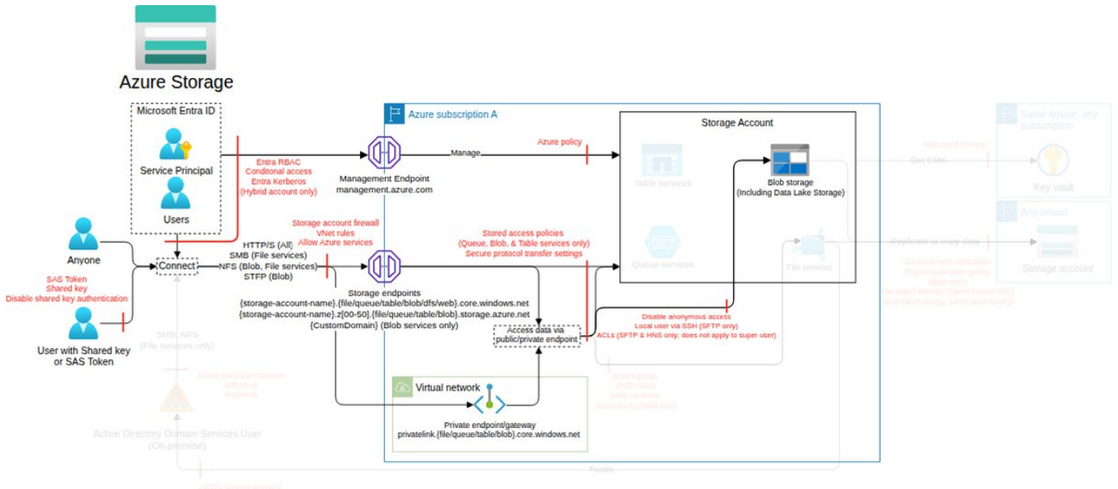
Action	IAM Permission
Create or update the properties of a local user associated with the storage account. Properties for NFSv3 enablement and extended Groups cannot be set with other properties.	Microsoft.Storage/storageAccounts/localUsers/write

Threat List

Name	CVSS
Credential access through accessing SMB Shared Key	Medium (6.9)
File share access through SMB Shared Key	Medium (4.8)
Persistent access to data by creating SFTP local user credentials	Low (3.5)

Credential access through accessing SMB Shared Key

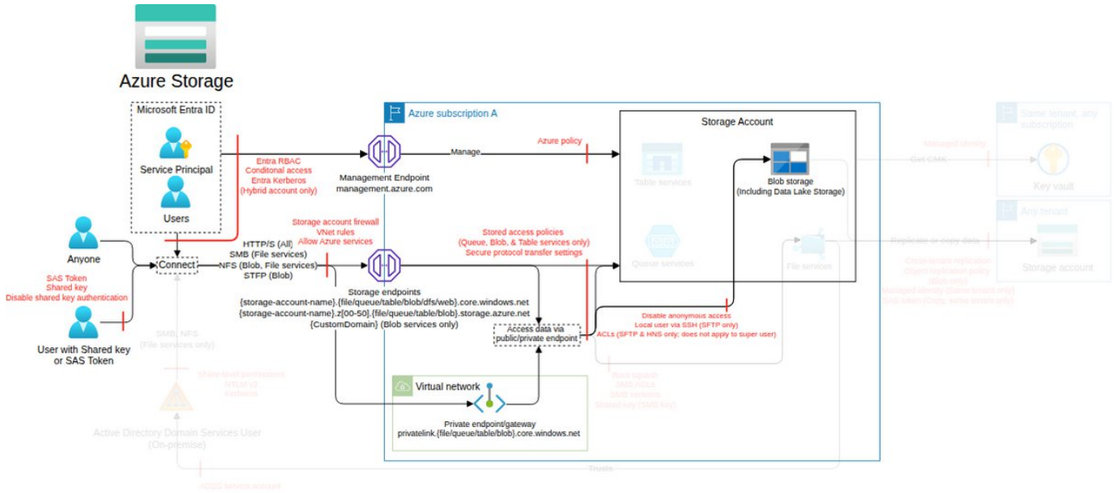
Threat Id	Storage.T64
Name	Credential access through accessing SMB Shared Key
Description	Azure file shares support SMB authentication via Shared Key (in the form of a password). An attacker can list this key through an API call, giving them full access to the file share.
Goal	Launch another attack
MITRE ATT&CK®	TA0006
CVSS	Medium (6.9)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/localUsers/listKeys/action" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C161 - Maintain a list of authorized local users, their permissions, and their authentication methods (e.g., password, SSH) for each hierarchical namespace with SFTP enabled. C162 - Ensure all local users and associated permissions and authentication methods are authorized.	High	3	-	-
CO21 - Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model C22 - Maintain a list of storage accounts that require hierarchical namespace (i.e., Data Lake Storage) and SSH enabled.	Medium	1	-	-

File share access through SMB Shared Key

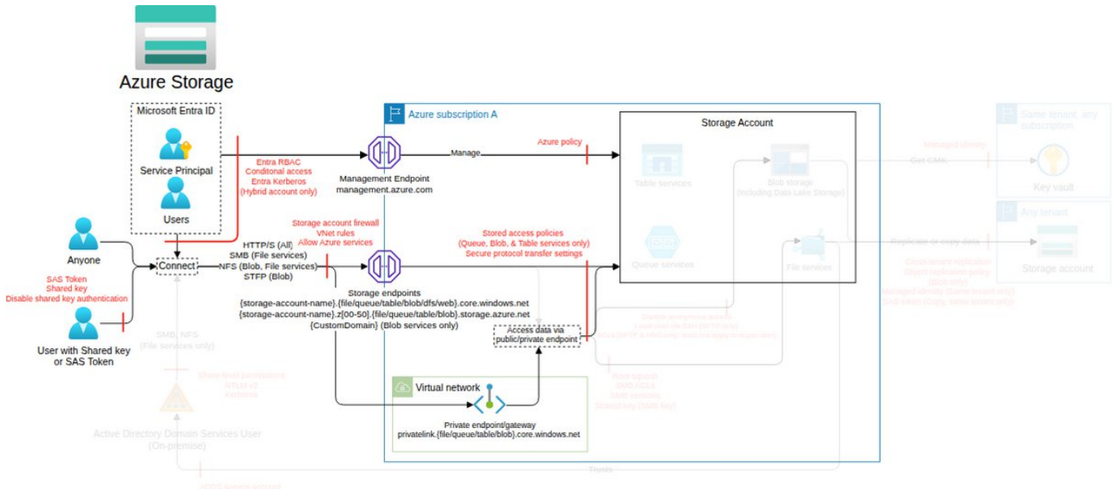
Threat Id	Storage.T65
Name	File share access through SMB Shared Key
Description	Azure file shares support SMB authentication via Shared Key (in the form of a password). An attacker can use this key to access and mount the file share, bypassing control plane API calls and logging.
Goal	Launch another attack
MITRE ATT&CK®	TA0001
CVSS	Medium (4.8)
IAM Access	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C161 - Maintain a list of authorized local users, their permissions, and their authentication methods (e.g., password, SSH) for each hierarchical namespace with SFTP enabled. C162 - Ensure all local users and associated permissions and authentication methods are authorized.	High	3	-	-
CO21 - Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model C22 - Maintain a list of storage accounts that require hierarchical namespace (i.e., Data Lake Storage) and SSH enabled.	Medium	1	-	-

Persistent access to data by creating SFTP local user credentials

Threat Id	Storage.T44
Name	Persistent access to data by creating SFTP local user credentials
Description	Storage accounts support SFTP and local accounts. An attacker can maintain persistence in a Storage account by creating SFTP local-user credentials.
Goal	Data theft
MITRE ATT&CK®	TA0010
CVSS	Low (3.5)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/localUsers/write" }

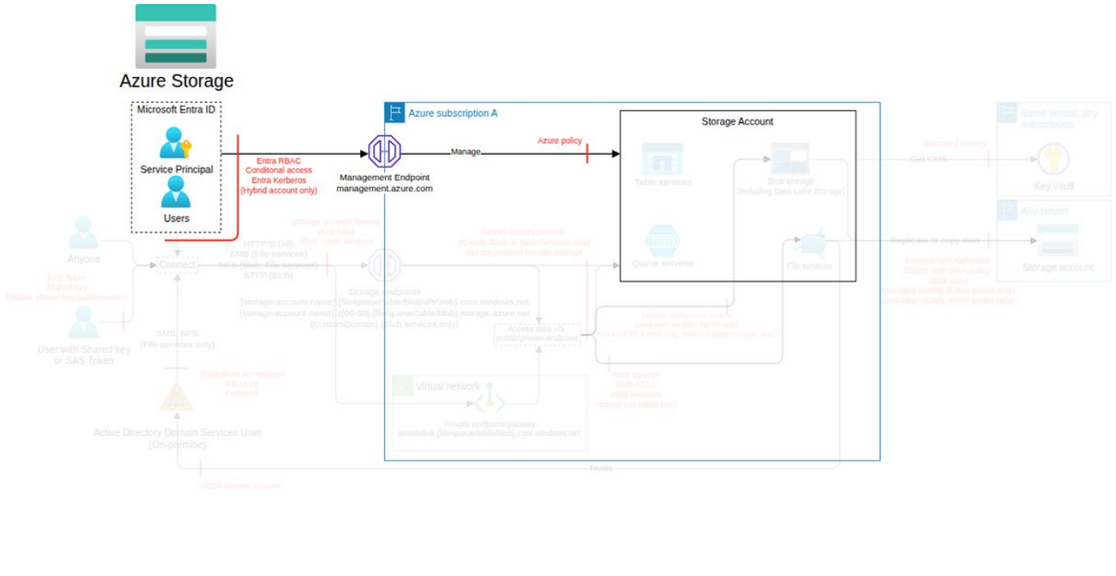


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO4 - Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) C2 - Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token). C149 - Ensure required blobs, file shares, queues, tables, and DFS are using authorized authentication methods. C161 - Maintain a list of authorized local users, their permissions, and their authentication methods (e.g., password, SSH) for each hierarchical namespace with SFTP enabled.	High	3	-	-
CO21 - Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model C22 - Maintain a list of storage accounts that require hierarchical namespace (i.e., Data Lake Storage) and SSH enabled. C111 - Maintain a list of Data Lake Storage accounts that require SFTP enabled. C114 - Ensure only storage accounts that require SFTP have it enabled. C115 - Prevent storage accounts that do not require SFTP from having it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/isSftpEnabled": true} in Deny mode).	Medium	3	1	-

Private endpoints *(subclass of Storage account, FC12)*

Azure Storage private endpoint is a network interface that enables secure, private connectivity between Azure Storage and virtual networks using Azure Private Link, preventing exposure to the public internet and enhancing security.

Data Flow Diagram (DFD)



Actions and IAM Permissions to deny the feature

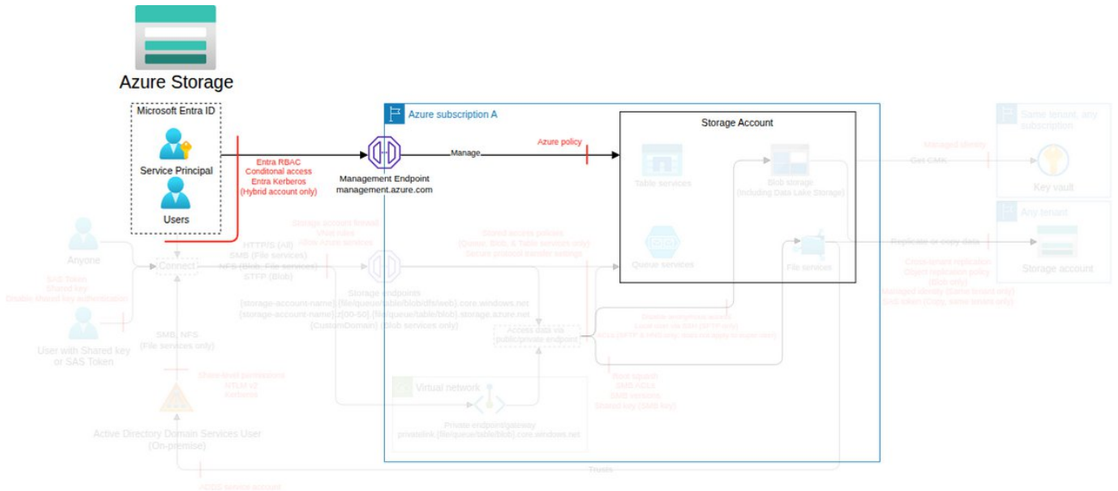
Action	IAM Permission
Update the state of specified private endpoint connection associated with the storage account.	Microsoft.Storage/storageAccounts/privateEndpointConnections/write

Threat List

Name	CVSS
Denial of Service by deleting private endpoint	Low (2.4)

Denial of Service by deleting private endpoint

Threat Id	Storage.T62
Name	Denial of Service by deleting private endpoint
Description	Azure Storage accounts support private endpoints as a way to access the service endpoints in a private network. An attacker can disable or delete the private endpoints, causing a Denial of Service.
Goal	Disruption of Service
MITRE ATT&CK®	TA0040
CVSS	Low (2.4)
IAM Access	{ "UNIQUE": "Microsoft.Storage/storageAccounts/privateEndpointConnections/delete" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
CO1 - Limit the IAM entities allowed to use the IAM actions required to execute attacks C1 - Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Very High	1	-	-
CO9 - Limit network access to storage account services with private endpoints C37 - Maintain a list of authorized private endpoints on storage accounts. C38 - Ensure only authorized private endpoints are configured on storage accounts.	Very High	2	-	-

Control Implementation

Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO1]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[Storage.C1] Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Request the list of authorized IAM principals with the permissions required to launch attacks, a list of Trusted Networks and PIM settings where applicable, its review process, and its review records.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC5 Storage.FC10 Storage.FC11 Storage.FC12	Storage.T1 (Very High) Storage.T2 (Very High) Storage.T4 (Very High) Storage.T5 (Very High) Storage.T7 (Very High) Storage.T8 (Very High) Storage.T9 (Very High) Storage.T10 (Very Low) Storage.T12 (Very High) Storage.T13 (Very High) Storage.T15 (Very High) Storage.T16 (Very High) Storage.T18 (Very High) Storage.T20 (Very High) Storage.T22 (Very High) Storage.T24 (Very High) Storage.T25 (Very High) Storage.T26 (Very High) Storage.T27 (Very High) Storage.T28 (Very High) Storage.T31 (Very High) Storage.T34 (Very High) Storage.T38 (Very High) Storage.T39 (Very High) Storage.T42 (Very High) Storage.T44 (Very High) Storage.T49 (Very High) Storage.T50 (Very High) Storage.T59 (Very High) Storage.T60 (Very High) Storage.T62 (Very High) Storage.T63 (Very High) Storage.T64 (Very High) Storage.T66 (Very High)	Very High

Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO4]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C2] Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token).	Request the list of storage accounts and their authorized authentication methods, its review process, and its review records.	Low	Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC5 Storage.FC11	Storage.T5 (Very Low) Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T15 (Very Low)	High

					Storage.T20 (Very Low) Storage.T27 (Very Low) Storage.T28 (Very Low) Storage.T31 (Very Low) Storage.T34 (Very Low) Storage.T44 (Very Low) Storage.T64 (Very Low) Storage.T65 (Very Low)	
Directive (COSO) Identify (NIST CSF)	[Storage.C6] Maintain a list of storage accounts that require public access to be enabled.	Request the list of required storage accounts with public access enabled, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T5 (Very Low) Storage.T50 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C7, depends on Storage.C6, assured by Storage.C9] Ensure only required storage accounts have public access enabled.	Request 1) the mechanism ensuring only required storage accounts have public access enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C8, depends on Storage.C6] Prevent the creation or update of non-required storage accounts with public access enabled (e.g., by using Azure built-in policy "Storage accounts should disable public network access" in Deny mode).	Modify a non-required storage account to have public access enabled; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C9] Verify non-required storage accounts do not have public access enabled (e.g., by using Azure built-in policy "Storage accounts should disable public network access" in Audit mode).	Modify a non-required storage account to have public access enabled; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C26, depends on Storage.C2] Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed permissions.	Request the list of storage accounts authorized to use SAS token authentication, its review process, and its review records.	Low	Storage.FC2 Storage.FC4 Storage.FC5	Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T27 (Very Low) Storage.T28 (Very Low) Storage.T31 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C27, depends on Storage.C26, assured by Storage.C28] Ensure SAS token authentication is enabled only for storage accounts that allow it.	Request 1) the mechanism ensuring only storage accounts that allow SAS token authentication have it enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts that allow SAS token authentication.	Low	Storage.FC2 Storage.FC4	Storage.T9 (Very Low) Storage.T12 (Medium) Storage.T31 (Low)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C28] Verify only storage accounts allowing SAS token authentication have it enabled (e.g., by using Azure built-in policy StorageAccountAllowSharedKeyAccess_Audit.json).	Enable SAS token authentication on a storage account that should not allow it; it should be detected.	Low	Storage.FC2 Storage.FC4	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C55] Maintain a list of blobs and containers that require anonymous access.	Request the list of authorized blobs and containers that require anonymous access, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T5 (Very Low) Storage.T50 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C56, depends on Storage.C55, assured by Storage.C59] Ensure anonymous access is set only for required blobs and containers.	Request 1) the mechanism ensuring only required blobs/containers are anonymously accessible, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Medium	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C57, depends on Storage.C55, assured by Storage.C59] Ensure only required blobs and containers are anonymously accessible (e.g., by using a custom Azure Policy on	Create or update a non-required blob or a container to be anonymously accessible; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium

	{"Microsoft.Storage/storageAccounts/blobServices/containers/publicAccess": "Blob"} in Deny mode).					
Assurance (COSO) Detect (NIST CSF)	[Storage.C59] Verify only required blobs or containers are anonymously accessible (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/containers/publicAccess": "Blob"} in Audit mode).	Create or update a non-required blob or a container to be anonymously accessible; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C81] Verify only the authorized authorization methods are set for authorized blobs, file shares, queues, tables, and DFS (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/protocolSettings.authenticationMethods[*]": ["SharedKey","AzureAD"]} in Audit mode).	Configure a blob, file share, queue, table, or DFS with an unauthorized authorization method; it should be detected.	Medium	Storage.FC3 Storage.FC11	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C90] Maintain a list of storage accounts that require static website hosting.	Request the list of storage accounts that require static website hosting, its review process, and its review records.	Low	Storage.FC2	Storage.T22 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C91, depends on Storage.C90, assured by Storage.C93] Ensure only storage accounts that require static website hosting have it enabled.	Request 1) the mechanism ensuring only required storage accounts have the static website hosting enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T22 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C92, depends on Storage.C90] Prevent storage accounts that do not require static website hosting from having it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/staticWebsite.enabled": true} in Deny mode).	Modify an existing storage account that does not require static website hosting to be enabled; it should be denied.	Medium	Storage.FC2	Storage.T22 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C93] Verify storage accounts that do not require static website hosting do not have it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/staticWebsite.enabled": true} in Audit mode).	Modify an existing storage account that does not require static website hosting to be enabled; it should be detected.	Medium	Storage.FC2	-	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C149, depends on Storage.C2, assured by Storage.C81] Ensure required blobs, file shares, queues, tables, and DFS are using authorized authentication methods.	Request 1) the mechanism ensuring blobs, file shares, queues, tables, and DFS use authorized authentication methods, 2) its records of execution for new storage account services, and 3) the plan to move any older storage account services.	Very Low	Storage.FC3 Storage.FC11	Storage.T20 (Medium) Storage.T44 (Medium)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C156, depends on Storage.C26, assured by Storage.C157] Ensure all stored access policy permissions are authorized on each container, file share, queue, and table.	Request 1) the mechanism ensuring all stored access policies and their permissions are authorized, 2) its records of execution for all new containers, file shares, queues, and tables, and 3) the plan to move any older containers, file shares, queues, and tables.	Low	Storage.FC4 Storage.FC5	Storage.T27 (Low) Storage.T28 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C157] Verify all stored access policy permissions are authorized (e.g., by using a custom Azure Policy with your allowedPermissions variable set to the permissions you've authorized in Audit mode).	Modify an existing stored access policy's permissions; it should be detected.	Low	Storage.FC4 Storage.FC5	-	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C161, depends on Storage.C22] Maintain a list of authorized local users, their	Request the list of authorized local users, their permissions, their authentication methods, its review	Low	Storage.FC11	Storage.T44 (Very Low) Storage.T64 (Very Low)	Medium

	permissions, and their authentication methods (e.g., password, SSH) for each hierarchical namespace with SFTP enabled.	process, and its review records.			Storage.T65 (Very Low)	
Directive (COSO) Protect (NIST CSF)	[Storage.C162, depends on Storage.C161, assured by Storage.C163] Ensure all local users and associated permissions and authentication methods are authorized.	Request 1) the mechanism ensuring all local users and associated permissions and authentication methods are authorized, 2) its records of execution for all new local users, and 3) the plan to move any older local users.	Low	Storage.FC11	Storage.T64 (Medium) Storage.T65 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C163] Verify all local users and associated permissions and authentication methods are authorized (e.g., by using a custom Azure Policy on "where": {"field": "Microsoft.Storage/storageAccounts/localUsers/permissionScopes[*].permissions", "notIn": "[parameters(\"allowedPermissions\")]"} in Audit mode).	Create a new local user; it should be detected.	Medium	Storage.FC11	-	Medium

Ensure backup, replication, and recovery capabilities for storage account services [Storage.CO5]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[Storage.C10, depends on Storage.C144, assured by Storage.C11] Ensure versioning is enabled on required containers.	Request 1) the mechanism ensuring versioning is enabled on required containers, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T7 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C11] Verify versioning is enabled on required containers (e.g., by using Azure built-in policy "Configure your Storage account to enable blob versioning" in Audit mode).	Remove versioning from a container; it should be detected.	Medium	Storage.FC2	-	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C12, depends on Storage.C145, assured by Storage.C13] Ensure snapshots are enabled for required file shares.	Request 1) the mechanism that ensures snapshots are enabled for required file shares, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T7 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C13] Verify snapshots are enabled for required file shares (e.g., by using a custom Azure Policy on {"properties.shareSnapshotEnabled": false} in Audit mode).	Disable snapshotting from a required file share; it should be detected.	Medium	Storage.FC2	-	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C15] Maintain a list of the blob storage containers that are required to have a minimum retention period enabled.	Request the list of storage account containers that have a minimum retention period according to requirements, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T25 (Very Low) Storage.T39 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C16, depends on Storage.C15, assured by Storage.C18] Ensure required storage accounts have the soft-delete feature for blobs enabled for the defined minimum retention period.	Request 1) the mechanism ensuring required storage accounts have soft-delete for blobs enabled for at least the defined minimum retention, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low)	Very Low
Preventative (COSO) Protect (NIST CSF)	[Storage.C17, depends on Storage.C15] Prevent the creation of required storage accounts without the blob soft-delete option enabled (e.g., by using a custom Azure Policy on	Create a required storage account without soft-delete for the blob; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T9 (High) Storage.T25 (Low) Storage.T39 (Very Low)	Medium

	{"Microsoft.Storage/storageAccounts/deleteRetentionPolicy.enabled": false} in Deny mode).					
Assurance (COSO) Detect (NIST CSF)	[Storage.C18] Verify required storage accounts have the blob soft-delete option enabled (e.g., by using custom Azure Policy in Audit mode).	Create a required storage account without soft-delete for the blob option; it should be detected.	Medium	Storage.FC2	-	Very Low
Directive (COSO) Protect (NIST CSF)	[Storage.C19, depends on Storage.C15, assured by Storage.C21] Ensure required storage accounts have the soft-delete option enabled for the containers.	Request 1) the mechanism ensuring required storage accounts have soft-delete for the container enabled, 2) its records of execution for all new required storage accounts, and 3) the plan to move any older required storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T25 (Low) Storage.T39 (Very Low)	Low
Preventative (COSO) Protect (NIST CSF)	[Storage.C20, depends on Storage.C15] Prevent the creation of containers without the soft-delete option enabled (e.g., by using a custom Azure Policy on "Microsoft.Storage/storageAccounts/blobServices/containers/softDelete" in Deny mode).	Create a container without soft-delete; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T9 (High) Storage.T25 (Low) Storage.T39 (Very Low)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C21] Verify required storage accounts have container soft delete enabled (e.g., by using custom Azure Policy in Audit mode).	Create a storage account without soft-delete for the container option; it should be detected.	Low	Storage.FC1 Storage.FC2	-	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C46, depends on Storage.C147] Ensure storage blobs are using Azure Backup, following the requirements in the Azure Backup ThreatModel.	Request 1) the mechanism ensuring storage blobs are using Azure Backup, 2) its records of execution for all new storage blobs, and 3) the plan to move any older storage blobs.	High	Storage.FC2	Storage.T7 (Medium) Storage.T9 (Medium) Storage.T12 (Medium)	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C47] Maintain a list of storage accounts that require cross-tenant replication and their allowed destination tenants.	Request the list of storage accounts that require cross-tenant replication and their allowed destination tenants, its review process, and its review records.	Low	Storage.FC1	Storage.T13 (Very Low) Storage.T42 (Very Low) Storage.T63 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C48, depends on Storage.C47, assured by Storage.C49] Ensure only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized.	Request 1) the mechanism that ensures only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized, 2) its records of execution for all new storage accounts, 3) the plan to move any older storage accounts.	Low	Storage.FC1	Storage.T13 (High) Storage.T42 (High) Storage.T63 (Medium)	High
Assurance (COSO) Detect (NIST CSF)	[Storage.C49] Verify only the storage accounts that require cross-tenant replication have it enabled (e.g., by using Azure built-in policy StorageAccountAllowCrossTenantReplication_Audit.json).	Create a storage account with cross-tenant replication enabled; it should be detected.	Medium	Storage.FC1	-	High
Directive (COSO) Identify (NIST CSF)	[Storage.C71] Maintain a list of storage accounts that require redundancy.	Request the list of storage accounts that require redundancy, its review process, and its review records.	Low	Storage.FC3	Storage.T60 (Very Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[Storage.C72, depends on Storage.C71, assured by Storage.C74] Ensure required storage accounts use redundancy.	Request 1) the mechanism ensuring required storage accounts use redundancy, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC3	Storage.T60 (Low)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C74] Verify required storage accounts use redundancy (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/sku.name": ["Standard_GRS","Standard_ZRS"]} in Audit mode).	Remove a redundancy configuration from a storage account; it should be detected.	Medium	Storage.FC3	-	Very Low
Directive (COSO)	[Storage.C75]	Request the list of authorized storage account regions	Low	Storage.FC1	Storage.T59 (Very Low)	Low

Identify (NIST CSF)	Maintain a list of authorized storage account regions that can be used for redundancy.	that are used for redundancy, its review process, and its review records.				
Directive (COSO) Protect (NIST CSF)	[Storage.C76, depends on Storage.C75, assured by Storage.C78] Ensure the authorized storage account region used for redundancy is configured.	Request 1) the mechanism ensuring only authorized regions for storage accounts are in use, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1	Storage.T59 (Medium)	Very Low
Preventative (COSO) Protect (NIST CSF)	[Storage.C77, depends on Storage.C75] Ensure only the authorized storage account region is set for redundancy (e.g., by using a custom Azure Policy on {"location": ["eastus","westeurope"]} in Deny mode).	Create a redundancy configuration on a storage account with an unauthorized region; it should be denied.	Medium	Storage.FC1	Storage.T59 (High)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C78] Verify only the authorized storage account region is set for redundancy (e.g., by using a custom Azure Policy with {"location": ["eastus","westeurope"]} in Audit mode).	Create a storage account with an unauthorized region; it should be detected.	Medium	Storage.FC1	-	Very Low
Directive (COSO) Identify (NIST CSF)	[Storage.C83] Define the minimum retention period for required file shares (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/deleteRetentionPolicy.days": 7} in Deny mode).	For each file share, request the minimum retention from deletion, its review process, and its review records.	Medium	Storage.FC3	Storage.T18 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C84, depends on Storage.C83, assured by Storage.C86] Ensure file shares have the soft-delete option enabled for at least the defined minimum retention period.	Request 1) the mechanism ensuring file shares have soft-delete enabled for at least the defined minimum retention, 2) its records of execution for all new file shares, and 3) the plan to move any older file shares.	Low	Storage.FC3	Storage.T18 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C85, depends on Storage.C83] Prevent the creation of file shares without the soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/shares/deleteRetentionPolicy.enabled": false} in Deny mode).	Create a file share without soft-delete; it should be denied.	Medium	Storage.FC3	Storage.T18 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C86] Verify all file shares have the soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/shares/deleteRetentionPolicy.enabled": false} in Audit mode).	Create a file share without soft-delete; it should be detected.	Medium	Storage.FC3	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C145] Maintain a list of Azure Files that require snapshots.	Request the list of Azure Files that require snapshots, its review process, and its review records.	Low	Storage.FC2	Storage.T7 (Very Low)	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C147] Maintain a list of storage blobs that require Azure Backup.	Request the list of storage blobs that require Azure Backup, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T13 (Very Low)	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C150] Maintain a list of authorized replication policies and their destination storage accounts.	Request the list of authorized replication policies and their destination storage accounts, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T13 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C151, depends on Storage.C150, assured by Storage.C152] Ensure replication policies and their destination storage accounts are authorized.	Request 1) the mechanism ensuring replication policies and their destination storage accounts are authorized, 2) its records of execution for all new replication policies, and 3) the plan to move any older replication policies.	Very Low	Storage.FC1	Storage.T13 (Low)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C152] Verify replication policies and their destination storage accounts are authorized (e.g., by using custom Azure	Add an unauthorized replication policy; it should be detected.	Medium	Storage.FC1	-	Medium

	Policy in Audit mode).					

Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO7]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C158] Maintain a list of authorized Access Control Lists (ACLs) on Data Lake Storage containers.	Request the list of authorized Access Control Lists (ACLs) on Data Lake Storage containers, its review process, and its review records.	Low	Storage.FC2	Storage.T66 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C159, depends on Storage.C158, assured by Storage.C160] Ensure all Access Control Lists (ACLs) on Data Lake Storage containers are authorized.	Request 1) the mechanism ensuring all Access Control Lists (ACLs) on Data Lake Storage containers are authorized, 2) its records of execution for all new ACLs, and 3) the plan to move any older ACLs.	Low	Storage.FC2	Storage.T66 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C160] Verify all Access Control Lists (ACLs) on Data Lake Storage containers are authorized (e.g., by using a custom Azure Policy on "where": {"field": "Microsoft.Storage/storageAccounts/blobServices/containers/acl[*].id", "notIn": "[parameters (\"authorizedPrincipals\")]"} in Audit mode).	Create a new ACL; it should be detected.	Medium	Storage.FC2	-	Medium

Enforce encryption in transit [Storage.CO8]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C98] Maintain a list of file shares that require NFS/SMB 2.1 enabled.	Request the list of file shares that require NFS/SMB 2.1 enabled, its review process, and its review records.	Low	Storage.FC3	Storage.T61 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C99, depends on Storage.C98, assured by Storage.C102] Ensure only file shares that require NFS/SMB 2.1 have it enabled.	Request 1) the mechanism ensuring only file shares that require NFS/SMB 2.1 have it enabled, 2) its records of execution for all new file shares, and 3) the plan to move any older file shares.	Very Low	Storage.FC3	Storage.T61 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C100, depends on Storage.C98] Prevent file shares that do not require NFS/SMB 2.1 from being enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb.protocolVersions[*]": ["SMB2.1"]} in Deny mode).	Modify an existing file share that does not require NFS/SMB 2.1 to use NFS/SMB 2.1; it should be denied.	Medium	Storage.FC3	Storage.T61 (High)	Medium
Detective (COSO) Detect (NIST CSF)	[Storage.C101] Monitor the creation or update of Azure Files NFS/SMB 2.1 and corresponding settings (e.g., using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly").	Modify or create a file share that does not require NFS/SMB 2.1 to use NFS/SMB 2.1; it should be detected.	Low	Storage.FC3	Storage.T61 (Very Low)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C102] Verify only file shares that require NFS/SMB 2.1 have it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb.protocolVersions[*]": ["SMB2.1"]} in Audit mode).	Modify an existing file share that does not require NFS/SMB 2.1 to use NFS/SMB 2.1; it should be detected.	Medium	Storage.FC3	-	Medium

Directive (COSO) Identify (NIST CSF)	[Storage.C120] Maintain a list of required file shares' security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only).	Request the list of required file share security protocol settings, its review process, and its review records.	Low	Storage.FC3	Storage.T15 (Very Low) Storage.T20 (Very Low) Storage.T60 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C121, depends on Storage.C120, assured by Storage.C123] Ensure required file shares' security protocol settings are set.	Request 1) the mechanism ensuring that the required security protocol settings for file shares in storage accounts are in use, 2) its records of execution for all new file shares, and 3) the plan to move any older file shares.	Low	Storage.FC3	Storage.T15 (Medium) Storage.T20 (Low) Storage.T60 (Medium)	Low
Preventative (COSO) Protect (NIST CSF)	[Storage.C122, depends on Storage.C120] Prevent security protocol settings from changing on required file shares (e.g., by using custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb": {"kerberosTicketEncryption":"AES256","channelEncryption":"Required"}} in Deny mode).	Modify a required file share's security protocol settings; it should be denied.	Medium	Storage.FC3	Storage.T20 (Low) Storage.T60 (High)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C123] Verify required file shares' security protocol settings are configured (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb": {"kerberosTicketEncryption":"AES256","channelEncryption":"Required"}} in Audit mode).	Modify a required file share's security protocol settings; it should be detected.	Medium	Storage.FC3	-	Low

Limit network access to storage account services with private endpoints [Storage.CO9]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C37] Maintain a list of authorized private endpoints on storage accounts.	Request the list of authorized private endpoints, its review process, and its review records.	Low	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC12	Storage.T1 (Very Low) Storage.T5 (Very Low) Storage.T12 (Very Low) Storage.T15 (Very Low) Storage.T31 (Very Low) Storage.T50 (Very Low) Storage.T62 (Very Low)	Very High
Directive (COSO) Protect (NIST CSF)	[Storage.C38, depends on Storage.C37, assured by Storage.C40] Ensure only authorized private endpoints are configured on storage accounts.	Request 1) the mechanism ensuring only authorized private endpoints are configured on storage accounts, 2) its records of execution for all private endpoints.	Low	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC12	Storage.T1 (Very High) Storage.T5 (Low) Storage.T12 (Medium) Storage.T15 (Low) Storage.T31 (Low) Storage.T50 (Medium) Storage.T62 (Medium)	Very High
Assurance (COSO) Detect (NIST CSF)	[Storage.C40] Verify only authorized private endpoints are configured on storage accounts (e.g., by using the built-in Azure Policy "Storage accounts should use Private Link" in Audit mode).	Configure an unauthorized private endpoint on a storage account; it should be detected.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC12	-	Very High
Directive (COSO) Identify (NIST CSF)	[Storage.C42] Maintain a list of authorized IPs that are permitted through each storage account firewall.	Request the list of authorized IPs, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T1 (Very Low) Storage.T5 (Very Low)	High

				Storage.FC3 Storage.FC4	Storage.T12 (Very Low) Storage.T15 (Very Low) Storage.T31 (Very Low) Storage.T50 (Very Low)	
Directive (COSO) Protect (NIST CSF)	[Storage.C43, depends on Storage.C42, assured by Storage.C45] Ensure each storage account firewall only allows authorized IPs.	Request 1) the mechanism ensuring firewall rules only allow authorized IP addresses, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4	Storage.T1 (High) Storage.T5 (High) Storage.T12 (High) Storage.T15 (High) Storage.T31 (High) Storage.T50 (High)	High
Preventative (COSO) Protect (NIST CSF)	[Storage.C44, depends on Storage.C42] Prevent access from unauthorized IPs by allowing only authorized IPs through the Azure Storage firewall (by using built-in Azure Policy "Storage accounts should restrict network access" in Deny mode).	Access from unauthorized IPs; it should be denied.	Very Low	Storage.FC1 Storage.FC3 Storage.FC4	Storage.T1 (Very Low) Storage.T15 (Medium) Storage.T31 (Medium) Storage.T50 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C45] Verify only authorized IPs are permitted through each storage account firewall (e.g., by using built-in Azure Policy "Storage accounts should restrict network access" in Audit mode).	Connect to a storage account from an unauthorized IP; it should be detected.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4	-	High

Enable enhanced monitoring and notifications for storage accounts [Storage.CO11]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C50] Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations.	Request the list of storage accounts that require diagnostic settings, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T8 (Very Low) Storage.T9 (Very Low) Storage.T10 (Very Low) Storage.T13 (Very Low) Storage.T42 (Very Low)	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C51, depends on Storage.C50, assured by Storage.C54] Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Request 1) the mechanism ensuring only authorized diagnostic settings destinations are enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T8 (Very Low) Storage.T9 (Very Low) Storage.T10 (Low) Storage.T13 (Very Low) Storage.T42 (Very Low)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C54] Verify storage accounts have diagnostic settings configured (e.g., by using built-in Azure Policy "Configure diagnostic settings for storage accounts to Log Analytics workspace" in Audit mode).	Create a storage account with unauthorized diagnostic settings options; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Very Low

Enforce encryption on data at rest and protect encryption keys [Storage.CO12]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C60] Maintain a list of authorized customer-managed keys	Request the list of authorized customer-managed keys used by storage accounts, its review process, and its	Low	Storage.FC1 Storage.FC2	Storage.T9 (Very Low) Storage.T38 (Very Low)	Medium

	used by storage accounts.	review records.				
Directive (COSO) Protect (NIST CSF)	[Storage.C61, depends on Storage.C60, assured by Storage.C65] Ensure only authorized customer-managed keys are configured for storage accounts.	Request 1) the mechanism ensuring only authorized customer-managed keys are used to encrypt each storage account, 2) its records of execution for all new storage accounts, and 3) the plan to move any older authorized storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T9 (Low) Storage.T38 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C63, depends on Storage.C61, assured by Storage.C65] Prevent storage accounts that require customer-managed keys from using service-managed keys (e.g., by using built-in Azure Policy "Storage accounts should use customer-managed key for encryption" in Deny mode).	Create a storage account requiring CMK with a service-managed key; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T9 (Medium) Storage.T38 (High)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C65] Verify only authorized customer-managed keys are configured for storage accounts (e.g., by using the built-in Azure Policy "Storage accounts should use customer-managed key for encryption" in Audit mode).	Modify a required storage account to use an unauthorized CMK; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Medium

Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO14]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C94] Maintain a list of authorized CORS per endpoint, trusted origins, and corresponding settings.	Request the list of authorized storage accounts with CORS trusted origins and corresponding settings, its review process, and its review records.	Low	Storage.FC1	Storage.T26 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C95, depends on Storage.C94, assured by Storage.C97] Ensure only authorized storage accounts have CORS-trusted origins and corresponding settings configured.	Request 1) the mechanism ensuring only authorized storage accounts have CORS trusted origins and corresponding settings configured, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1	Storage.T26 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C96, depends on Storage.C94] Prevent unauthorized storage accounts from using CORS trusted origins and corresponding settings (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/cors.allowedOrigins[*]": ["https://myapp.contoso.com"]} in Deny mode).	Create a storage account with untrusted CORS settings; it should be denied.	Medium	Storage.FC1	Storage.T26 (High)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C97] Verify only authorized CORS trusted origins and corresponding settings are configured (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/cors.allowedOrigins[*]": ["https://myapp.contoso.com"]} in Audit mode).	Create a storage account with untrusted CORS settings; it should be detected.	Medium	Storage.FC1	-	Medium

Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO21]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority

Directive (COSO) Identify (NIST CSF)	[Storage.C22, depends on Storage.C2] Maintain a list of storage accounts that require hierarchical namespace (i.e., Data Lake Storage) and SSH enabled.	Request the list of storage accounts that require hierarchical namespace, its review process, and its review records.	Low	Storage.FC2 Storage.FC11	Storage.T7 (Very Low) Storage.T44 (Very Low) Storage.T64 (Very Low) Storage.T65 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C23, depends on Storage.C22, assured by Storage.C24] Ensure all required storage accounts have hierarchical namespace (i.e., Data Lake Storage) enabled.	Request 1) the mechanism ensuring required storage accounts have hierarchical namespace enabled, 2) its records of execution for all new required storage accounts, 3) the plan to move any older storage accounts with hierarchical namespace.	Low	Storage.FC2	Storage.T7 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C24] Verify only required storage accounts have the hierarchical namespace (HNS) option enabled (e.g., by using a custom Azure Policy on {"isHnsEnabled": "true"} in Audit mode).	Create a non-required storage account with the hierarchical namespace (HNS) option enabled; it should be detected.	Medium	Storage.FC2	-	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C111, depends on Storage.C22] Maintain a list of Data Lake Storage accounts that require SFTP enabled.	Request the list of storage accounts that require SFTP, its review process, and its review records.	Low	Storage.FC11	Storage.T44 (Very Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[Storage.C114, depends on Storage.C111, assured by Storage.C116] Ensure only storage accounts that require SFTP have it enabled.	Request 1) the mechanism ensuring storage accounts that require SFTP have it enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Very Low	Storage.FC11	Storage.T44 (Low)	Very Low
Preventative (COSO) Protect (NIST CSF)	[Storage.C115, depends on Storage.C111] Prevent storage accounts that do not require SFTP from having it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/isSftpEnabled": true} in Deny mode).	Modify a storage account that does not require SFTP to use SFTP; it should be denied.	Medium	Storage.FC11	Storage.T44 (Medium)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C116] Verify only storage accounts that require SFTP have it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/isSftpEnabled": true} in Audit mode).	Modify a storage account that does not require SFTP to use SFTP; it should be detected.	Medium	Storage.FC11	-	Very Low

Protect the integrity of blob storage data from unauthorized changes [Storage.CO24]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[Storage.C32] Maintain a list of storage container blobs that require immutability and soft delete.	Request the list of storage container blobs that require immutability, its review process, and its review records.	Low	Storage.FC2	Storage.T7 (Very Low) Storage.T8 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C33, depends on Storage.C32, assured by Storage.C146] Ensure required storage container blobs have immutability and soft delete enabled.	Request 1) the mechanism ensuring that required storage container blobs have immutability enabled, 2) its records of execution for all new storage container blobs, and 3) the plan to move any older storage container blobs.	Low	Storage.FC2	Storage.T8 (Very High) Storage.T9 (Very High) Storage.T12 (Medium)	High
Directive (COSO) Identify (NIST CSF)	[Storage.C107] Maintain the list of storage accounts that should require read-only and/or delete locks.	Request the list of storage accounts that require read-only and/or delete locks, its review process, and its review records.	Low	Storage.FC1 Storage.FC3	Storage.T4 (Very Low) Storage.T18 (Very Low) Storage.T63 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C108, depends on Storage.C107, assured by Storage.C109] Ensure only required storage accounts have read-only	Request 1) the mechanism ensuring required storage accounts have read-only and/or delete locks applied, 2)	Very Low	Storage.FC1 Storage.FC3	Storage.T4 (High) Storage.T18 (Very High)	High

	and/or delete locks applied.	its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.			Storage.T63 (High)	
Assurance (COSO) Detect (NIST CSF)	[Storage.C109] Verify required storage accounts have read-only and/or delete locks applied (e.g., by using built-in Azure Policy "Resource locks should be applied" in Audit mode).	Remove a read-only or delete lock from a storage account; it should be detected.	Medium	Storage.FC1 Storage.FC3	-	High
Preventative (COSO) Detect (NIST CSF)	[Storage.C110] Prevent modification or deletion of required storage accounts by using a resource lock set to read-only and/or delete, using the Azure Resource Manager ThreatModel.	Modify or delete a required storage account; it should be denied.	Very Low	Storage.FC1 Storage.FC2 Storage.FC3	Storage.T12 (Very High) Storage.T18 (High) Storage.T63 (Very High)	High
Directive (COSO) Identify (NIST CSF)	[Storage.C144] Maintain a list of storage account blobs that require versioning and blob change feed to be enabled.	Request the list of storage account blobs that require versioning and blob change feed enabled, along with its review process and review records.	Low	Storage.FC2	Storage.T7 (Very Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C146] Verify required storage container blobs have immutability and soft delete enabled (e.g., by using built-in Azure Policy "Immutable blob storage should be enabled" in Audit mode).	Turn off immutability on a storage container blob that requires it to be enabled; it should be detected.	Low	Storage.FC2	-	High

Compliance Mapping

PCI DSS v4

PCI DSS v4	Control Objectives	Controls				
		Very High	High	Medium	Low	Very Low
1.1 1.2.1	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO8] Enforce encryption in transit [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C156 Storage.C157 Storage.C121 Storage.C122 Storage.C123	Storage.C101
1.2.3	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
1.2.4 1.2.5	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45 Storage.C32 Storage.C33	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27	Storage.C156 Storage.C157 Storage.C144	-

	storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes		Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C44 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
1.2.6	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
1.2.7	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163	Storage.C156 Storage.C157 Storage.C50 Storage.C144	Storage.C51 Storage.C54

				Storage.C158 Storage.C159 Storage.C160 Storage.C44 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
1.2.8	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
1.2.10	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1 Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24 Storage.C144	Storage.C111 Storage.C114 Storage.C115 Storage.C116
1.3	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-

1.3.1 1.3.2	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO8] Enforce encryption in transit [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C156 Storage.C157 Storage.C121 Storage.C122 Storage.C123	Storage.C101
1.3.3	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
1.4	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93	Storage.C156 Storage.C157	-

				Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
1.4.1	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
1.4.2	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44	Storage.C50	Storage.C51 Storage.C54
1.4.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues)	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163	Storage.C156 Storage.C157	-
1.4.4	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
1.4.5	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28	Storage.C156 Storage.C157 Storage.C144	-

			Storage.C146	Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
1.5 1.5.1 2.2.1	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
2.2.2	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO8] Enforce encryption in transit	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43	Storage.C6 Storage.C7 Storage.C8	Storage.C156 Storage.C157 Storage.C121	Storage.C101

	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts		Storage.C45	Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C122 Storage.C123	
2.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO8] Enforce encryption in transit [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C98 Storage.C99	Storage.C156 Storage.C157 Storage.C121 Storage.C122 Storage.C123 Storage.C23 Storage.C24	Storage.C101 Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C100 Storage.C102 Storage.C120 Storage.C22		
2.3.1	[Storage.CO8] Enforce encryption in transit [Storage.CO12] Enforce encryption on data at rest and protect encryption keys	-	-	Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C60 Storage.C61 Storage.C63 Storage.C65	Storage.C121 Storage.C122 Storage.C123	Storage.C101
2.3.2	[Storage.CO12] Enforce encryption on data at rest and protect encryption keys	-	-	Storage.C60 Storage.C61 Storage.C63 Storage.C65	-	-
3.3.2	[Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	-	Storage.C144	-
3.5.1	[Storage.CO12] Enforce encryption on data at rest and protect encryption keys	-	-	Storage.C60 Storage.C61 Storage.C63 Storage.C65	-	-
3.5.1.1 3.5.1.2 3.5.1.3 3.6.1 3.6.1.1 3.6.1.2 3.6.1.3 3.6.1.4 3.7.1 3.7.2 3.7.3 3.7.4	[Storage.CO8] Enforce encryption in transit [Storage.CO12] Enforce encryption on data at rest and protect encryption keys	-	-	Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C60 Storage.C61 Storage.C63 Storage.C65	Storage.C121 Storage.C122 Storage.C123	Storage.C101
3.7.5	[Storage.CO12] Enforce encryption on data at rest and protect encryption keys	-	-	Storage.C60 Storage.C61 Storage.C63 Storage.C65	-	-
3.7.6 3.7.7 3.7.9	[Storage.CO8] Enforce encryption in transit	-	-	Storage.C98 Storage.C99 Storage.C100	Storage.C121 Storage.C122 Storage.C123	Storage.C101

				Storage.C102 Storage.C120		
4.1 4.2.1	[Storage.CO12] Enforce encryption on data at rest and protect encryption keys	-	-	Storage.C60 Storage.C61 Storage.C63 Storage.C65	-	-
4.2.1.1	[Storage.CO8] Enforce encryption in transit	-	-	Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120	Storage.C121 Storage.C122 Storage.C123	Storage.C101
4.2.1.2 4.2.2	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
6.5.2	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92	Storage.C156 Storage.C157 Storage.C144	-

				Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
6.5.6	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24 Storage.C144	Storage.C111 Storage.C114 Storage.C115 Storage.C116
7.1 7.2	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59	Storage.C156 Storage.C157 Storage.C23 Storage.C24 Storage.C144	Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C94 Storage.C95 Storage.C96 Storage.C97 Storage.C22		
7.2.1 7.2.2	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24 Storage.C144	Storage.C111 Storage.C114 Storage.C115 Storage.C116
7.2.3	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks	Storage.C1	-	-	-	-
7.2.4	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56	Storage.C156 Storage.C157 Storage.C144	-

				Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
7.2.5	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C94 Storage.C95 Storage.C96 Storage.C97 Storage.C22	Storage.C156 Storage.C157 Storage.C50 Storage.C23 Storage.C24 Storage.C144	Storage.C51 Storage.C54 Storage.C111 Storage.C114 Storage.C115 Storage.C116
7.2.6	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26	Storage.C156 Storage.C157 Storage.C23 Storage.C24 Storage.C144	Storage.C111 Storage.C114 Storage.C115 Storage.C116

	[Storage.CO24] Protect the integrity of blob storage data from unauthorized changes		Storage.C109 Storage.C110 Storage.C146	Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22		
7.3 7.3.1 7.3.2 7.3.3	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.1 8.2	[Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model	-	-	Storage.C158 Storage.C159 Storage.C160	-	-
8.2.1	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22		
8.2.2	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160	Storage.C156 Storage.C157	-
8.2.3	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22		
8.2.4	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160	Storage.C156 Storage.C157	-
8.2.6	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22		
8.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.3.1	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO8] Enforce encryption in transit [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93	Storage.C156 Storage.C157 Storage.C121 Storage.C122 Storage.C123 Storage.C144	Storage.C101

				Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
8.3.2	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.3.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22		
8.3.5 8.3.6 8.3.7	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.3.8 8.3.9	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57	Storage.C156 Storage.C157	-

				Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160		
8.3.10	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.3.10.1 8.3.11	[Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model	-	-	Storage.C158 Storage.C159 Storage.C160	-	-
8.4 8.4.1 8.4.2 8.4.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59	Storage.C156 Storage.C157 Storage.C144	-

				Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
8.5	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.5.1	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28	Storage.C156 Storage.C157 Storage.C144	-

			Storage.C146	Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
8.6	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C94 Storage.C95 Storage.C96 Storage.C97 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24 Storage.C144	Storage.C111 Storage.C114 Storage.C115 Storage.C116
8.6.1	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model	-	Storage.C2	Storage.C6 Storage.C7 Storage.C8	Storage.C156 Storage.C157 Storage.C23	Storage.C111 Storage.C114 Storage.C115

	[Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model			Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C24	Storage.C116
8.6.2 8.6.3	[Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	-	Storage.C144	-
9.4 9.4.1	[Storage.CO5] Ensure backup, replication, and recovery capabilities for storage account services	-	Storage.C47 Storage.C48 Storage.C49	Storage.C15 Storage.C17 Storage.C20 Storage.C83 Storage.C84 Storage.C85 Storage.C86 Storage.C150 Storage.C151 Storage.C152	Storage.C10 Storage.C11 Storage.C12 Storage.C13 Storage.C19 Storage.C21 Storage.C46 Storage.C75 Storage.C77 Storage.C145 Storage.C147	Storage.C16 Storage.C18 Storage.C71 Storage.C72 Storage.C74 Storage.C76 Storage.C78
9.4.1.1 9.4.1.2	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44	Storage.C50	Storage.C51 Storage.C54
10.1	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to	Storage.C1 Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45 Storage.C32 Storage.C33 Storage.C107 Storage.C108	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55	Storage.C156 Storage.C157 Storage.C50 Storage.C23 Storage.C24 Storage.C144	Storage.C51 Storage.C54 Storage.C111 Storage.C114 Storage.C115 Storage.C116

	storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes		Storage.C109 Storage.C110 Storage.C146	Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C44 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97 Storage.C22		
10.2	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C1	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C60 Storage.C61 Storage.C63 Storage.C65	Storage.C156 Storage.C157 Storage.C50 Storage.C23 Storage.C24 Storage.C144	Storage.C51 Storage.C54 Storage.C111 Storage.C114 Storage.C115 Storage.C116

				Storage.C94 Storage.C95 Storage.C96 Storage.C97 Storage.C22		
10.2.1 10.2.1.1 10.2.1.2 10.2.1.3 10.2.1.4 10.2.1.5 10.2.1.6 10.2.1.7 10.2.2	[Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	-	-	-	Storage.C50	Storage.C51 Storage.C54
10.3 10.3.1 10.3.2 10.3.3	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44	Storage.C50	Storage.C51 Storage.C54
10.3.4 10.4 10.4.1 10.4.1.1 10.4.2 10.4.2.1 10.4.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	-	Storage.C2 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C156 Storage.C157 Storage.C50 Storage.C144	Storage.C51 Storage.C54
10.6	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs,	Storage.C37	Storage.C2	Storage.C6	Storage.C156	Storage.C51

10.6.1 10.6.2 10.6.3	queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C44 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C157 Storage.C50 Storage.C144	Storage.C54
10.7 10.7.1 10.7.2 10.7.3	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO8] Enforce encryption in transit [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO12] Enforce encryption on data at rest and protect encryption keys [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts [Storage.CO24] Protect the integrity of blob storage data from unauthorized changes	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45 Storage.C32 Storage.C33 Storage.C107 Storage.C108 Storage.C109 Storage.C110 Storage.C146	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158	Storage.C156 Storage.C157 Storage.C121 Storage.C122 Storage.C123 Storage.C50 Storage.C144	Storage.C101 Storage.C51 Storage.C54

				Storage.C159 Storage.C160 Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C44 Storage.C60 Storage.C61 Storage.C63 Storage.C65 Storage.C94 Storage.C95 Storage.C96 Storage.C97		
11.2	[Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO8] Enforce encryption in transit [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C2 Storage.C42 Storage.C43 Storage.C45	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120 Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C156 Storage.C157 Storage.C121 Storage.C122 Storage.C123	Storage.C101
11.2.1 11.2.2	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-

11.4.5 11.4.6	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44	Storage.C50	Storage.C51 Storage.C54
11.5	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	Storage.C50	Storage.C51 Storage.C54
11.5.1	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44	Storage.C50	Storage.C51 Storage.C54
11.5.1.1 11.5.2	[Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	-	-	Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
12.4.2	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
12.5.2	[Storage.CO8] Enforce encryption in transit	-	-	Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120	Storage.C121 Storage.C122 Storage.C123	Storage.C101
12.10.1	[Storage.CO8] Enforce encryption in transit [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	-	-	Storage.C98 Storage.C99 Storage.C100 Storage.C102 Storage.C120	Storage.C121 Storage.C122 Storage.C123 Storage.C50	Storage.C101 Storage.C51 Storage.C54
12.10.5	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	-	Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C50 Storage.C23 Storage.C24	Storage.C51 Storage.C54 Storage.C111 Storage.C114 Storage.C115 Storage.C116
15.1	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
A1.1.4	[Storage.CO8] Enforce encryption in transit	-	-	Storage.C98 Storage.C99 Storage.C100 Storage.C102	Storage.C121 Storage.C122 Storage.C123	Storage.C101

				Storage.C120		
A2.1 A2.1.1 A2.1.2	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO14] Restrict and manage external websites (origins) that can make browser-based requests to storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44 Storage.C94 Storage.C95 Storage.C96 Storage.C97	-	-
A3.2.1 A3.2.4	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1 Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C158 Storage.C159 Storage.C160 Storage.C44 Storage.C22	Storage.C50 Storage.C23 Storage.C24	Storage.C51 Storage.C54 Storage.C111 Storage.C114 Storage.C115 Storage.C116
A3.2.6.1	[Storage.CO9] Limit network access to storage account services with private endpoints [Storage.CO11] Enable enhanced monitoring and notifications for storage accounts	Storage.C37 Storage.C38 Storage.C40	Storage.C42 Storage.C43 Storage.C45	Storage.C44	Storage.C50	Storage.C51 Storage.C54
A3.3.1	[Storage.CO1] Limit the IAM entities allowed to use the IAM actions required to execute attacks [Storage.CO4] Restrict access to storage accounts and their services (e.g., Azure Files, containers, blobs, queues) [Storage.CO7] Restrict access to Data Lake Storage containers by integrating ACLs into the IAM Operating Model [Storage.CO21] Restrict access to Data Lake Storage, including SFTP, by integrating the IAM Operating Model	Storage.C1	Storage.C2	Storage.C6 Storage.C7 Storage.C8 Storage.C9 Storage.C26 Storage.C27 Storage.C28 Storage.C55 Storage.C56 Storage.C57 Storage.C59 Storage.C81 Storage.C90 Storage.C91 Storage.C92 Storage.C93 Storage.C149 Storage.C161 Storage.C162 Storage.C163 Storage.C158 Storage.C159 Storage.C160 Storage.C22	Storage.C156 Storage.C157 Storage.C23 Storage.C24	Storage.C111 Storage.C114 Storage.C115 Storage.C116

Appendixes

Appendix 1 - Prioritized list for control implementation

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[Storage.C1] Limit and monitor the access to the IAM actions required to perform attacks using Azure RBAC and local privileges, limiting them to Trusted Networks with Conditional Access and Just-in-Time access using Privileged Identity Management when possible, following the Entra ID, Azure Resource Manager, and Azure Management ThreatModels.	Request the list of authorized IAM principals with the permissions required to launch attacks, a list of Trusted Networks and PIM settings where applicable, its review process, and its review records.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC5 Storage.FC10 Storage.FC11 Storage.FC12	Storage.T1 (Very High) Storage.T2 (Very High) Storage.T4 (Very High) Storage.T5 (Very High) Storage.T7 (Very High) Storage.T8 (Very High) Storage.T9 (Very High) Storage.T10 (Very Low) Storage.T12 (Very High) Storage.T13 (Very High) Storage.T15 (Very High) Storage.T16 (Very High) Storage.T18 (Very High) Storage.T20 (Very High) Storage.T22 (Very High) Storage.T24 (Very High) Storage.T25 (Very High) Storage.T26 (Very High) Storage.T27 (Very High) Storage.T28 (Very High) Storage.T31 (Very High) Storage.T34 (Very High) Storage.T38 (Very High) Storage.T39 (Very High) Storage.T42 (Very High) Storage.T44 (Very High) Storage.T49 (Very High) Storage.T50 (Very High) Storage.T59 (Very High) Storage.T60 (Very High) Storage.T62 (Very High) Storage.T63 (Very High) Storage.T64 (Very High) Storage.T66 (Very High)	Very High
Directive (COSO) Identify (NIST CSF)	[Storage.C37] Maintain a list of authorized private endpoints on storage accounts.	Request the list of authorized private endpoints, its review process, and its review records.	Low	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC12	Storage.T1 (Very Low) Storage.T5 (Very Low) Storage.T12 (Very Low) Storage.T15 (Very Low) Storage.T31 (Very Low) Storage.T50 (Very Low) Storage.T62 (Very Low)	Very High
Directive (COSO) Protect (NIST CSF)	[Storage.C38, depends on Storage.C37, assured by Storage.C40] Ensure only authorized private endpoints are configured on storage accounts.	Request 1) the mechanism ensuring only authorized private endpoints are configured on storage accounts, 2) its records of execution for all private endpoints.	Low	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4	Storage.T1 (Very High) Storage.T5 (Low) Storage.T12 (Medium) Storage.T15 (Low)	Very High

				Storage.FC12	Storage.T31 (Low) Storage.T50 (Medium) Storage.T62 (Medium)	
Assurance (COSO) Detect (NIST CSF)	[Storage.C40] Verify only authorized private endpoints are configured on storage accounts (e.g., by using the built-in Azure Policy "Storage accounts should use Private Link" in Audit mode).	Configure an unauthorized private endpoint on a storage account; it should be detected.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC12	-	Very High
Directive (COSO) Identify (NIST CSF)	[Storage.C2] Maintain a list of storage accounts and their authorized authentication methods enabled according to requirements (e.g., Entra ID, SAS token).	Request the list of storage accounts and their authorized authentication methods, its review process, and its review records.	Low	Storage.FC2 Storage.FC3 Storage.FC4 Storage.FC5 Storage.FC11	Storage.T5 (Very Low) Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T15 (Very Low) Storage.T20 (Very Low) Storage.T27 (Very Low) Storage.T28 (Very Low) Storage.T31 (Very Low) Storage.T34 (Very Low) Storage.T44 (Very Low) Storage.T64 (Very Low) Storage.T65 (Very Low)	High
Directive (COSO) Identify (NIST CSF)	[Storage.C47] Maintain a list of storage accounts that require cross-tenant replication and their allowed destination tenants.	Request the list of storage accounts that require cross-tenant replication and their allowed destination tenants, its review process, and its review records.	Low	Storage.FC1	Storage.T13 (Very Low) Storage.T42 (Very Low) Storage.T63 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C48, depends on Storage.C47, assured by Storage.C49] Ensure only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized.	Request 1) the mechanism that ensures only required storage accounts have cross-tenant replication enabled and the destination storage accounts are authorized, 2) its records of execution for all new storage accounts, 3) the plan to move any older storage accounts.	Low	Storage.FC1	Storage.T13 (High) Storage.T42 (High) Storage.T63 (Medium)	High
Assurance (COSO) Detect (NIST CSF)	[Storage.C49] Verify only the storage accounts that require cross-tenant replication have it enabled (e.g., by using Azure built-in policy StorageAccountAllowCrossTenantReplication_Audit.json).	Create a storage account with cross-tenant replication enabled; it should be detected.	Medium	Storage.FC1	-	High
Directive (COSO) Identify (NIST CSF)	[Storage.C42] Maintain a list of authorized IPs that are permitted through each storage account firewall.	Request the list of authorized IPs, its review process, and its review records.	Low	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4	Storage.T1 (Very Low) Storage.T5 (Very Low) Storage.T12 (Very Low) Storage.T15 (Very Low) Storage.T31 (Very Low) Storage.T50 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C43, depends on Storage.C42, assured by Storage.C45] Ensure each storage account firewall only allows authorized IPs.	Request 1) the mechanism ensuring firewall rules only allow authorized IP addresses, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4	Storage.T1 (High) Storage.T5 (High) Storage.T12 (High) Storage.T15 (High) Storage.T31 (High) Storage.T50 (High)	High
Assurance (COSO) Detect (NIST CSF)	[Storage.C45] Verify only authorized IPs are permitted through each storage account firewall (e.g., by using built-in Azure Policy "Storage accounts should restrict network	Connect to a storage account from an unauthorized IP; it should be detected.	Medium	Storage.FC1 Storage.FC2 Storage.FC3 Storage.FC4	-	High

	access" in Audit mode).					
Directive (COSO) Identify (NIST CSF)	[Storage.C32] Maintain a list of storage container blobs that require immutability and soft delete.	Request the list of storage container blobs that require immutability, its review process, and its review records.	Low	Storage.FC2	Storage.T7 (Very Low) Storage.T8 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C33, depends on Storage.C32, assured by Storage.C146] Ensure required storage container blobs have immutability and soft delete enabled.	Request 1) the mechanism ensuring that required storage container blobs have immutability enabled, 2) its records of execution for all new storage container blobs, and 3) the plan to move any older storage container blobs.	Low	Storage.FC2	Storage.T8 (Very High) Storage.T9 (Very High) Storage.T12 (Medium)	High
Directive (COSO) Identify (NIST CSF)	[Storage.C107] Maintain the list of storage accounts that should require read-only and/or delete locks.	Request the list of storage accounts that require read-only and/or delete locks, its review process, and its review records.	Low	Storage.FC1 Storage.FC3	Storage.T4 (Very Low) Storage.T18 (Very Low) Storage.T63 (Very Low)	High
Directive (COSO) Protect (NIST CSF)	[Storage.C108, depends on Storage.C107, assured by Storage.C109] Ensure only required storage accounts have read-only and/or delete locks applied.	Request 1) the mechanism ensuring required storage accounts have read-only and/or delete locks applied, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Very Low	Storage.FC1 Storage.FC3	Storage.T4 (High) Storage.T18 (Very High) Storage.T63 (High)	High
Assurance (COSO) Detect (NIST CSF)	[Storage.C109] Verify required storage accounts have read-only and/or delete locks applied (e.g., by using built-in Azure Policy "Resource locks should be applied" in Audit mode).	Remove a read-only or delete lock from a storage account; it should be detected.	Medium	Storage.FC1 Storage.FC3	-	High
Preventative (COSO) Detect (NIST CSF)	[Storage.C110] Prevent modification or deletion of required storage accounts by using a resource lock set to read-only and/or delete, using the Azure Resource Manager ThreatModel.	Modify or delete a required storage account; it should be denied.	Very Low	Storage.FC1 Storage.FC2 Storage.FC3	Storage.T12 (Very High) Storage.T18 (High) Storage.T63 (Very High)	High
Assurance (COSO) Detect (NIST CSF)	[Storage.C146] Verify required storage container blobs have immutability and soft delete enabled (e.g., by using built-in Azure Policy "Immutable blob storage should be enabled" in Audit mode).	Turn off immutability on a storage container blob that requires it to be enabled; it should be detected.	Low	Storage.FC2	-	High
Directive (COSO) Identify (NIST CSF)	[Storage.C6] Maintain a list of storage accounts that require public access to be enabled.	Request the list of required storage accounts with public access enabled, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T5 (Very Low) Storage.T50 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C7, depends on Storage.C6, assured by Storage.C9] Ensure only required storage accounts have public access enabled.	Request 1) the mechanism ensuring only required storage accounts have public access enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C8, depends on Storage.C6] Prevent the creation or update of non-required storage accounts with public access enabled (e.g., by using Azure built-in policy "Storage accounts should disable public network access" in Deny mode).	Modify a non-required storage account to have public access enabled; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C9] Verify non-required storage accounts do not have public access enabled (e.g., by using Azure built-in policy "Storage accounts should disable public network access" in Audit mode).	Modify a non-required storage account to have public access enabled; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C26, depends on Storage.C2] Maintain a list of storage accounts that allow SAS token authentication, its allowed services, and its allowed	Request the list of storage accounts authorized to use SAS token authentication, its review process, and its review records.	Low	Storage.FC2 Storage.FC4 Storage.FC5	Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T27 (Very Low)	Medium

	permissions.				Storage.T28 (Very Low) Storage.T31 (Very Low)	
Directive (COSO) Protect (NIST CSF)	[Storage.C27, depends on Storage.C26, assured by Storage.C28] Ensure SAS token authentication is enabled only for storage accounts that allow it.	Request 1) the mechanism ensuring only storage accounts that allow SAS token authentication have it enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts that allow SAS token authentication.	Low	Storage.FC2 Storage.FC4	Storage.T9 (Very Low) Storage.T12 (Medium) Storage.T31 (Low)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C28] Verify only storage accounts allowing SAS token authentication have it enabled (e.g., by using Azure built-in policy StorageAccountAllowSharedKeyAccess_Audit.json).	Enable SAS token authentication on a storage account that should not allow it; it should be detected.	Low	Storage.FC2 Storage.FC4	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C55] Maintain a list of blobs and containers that require anonymous access.	Request the list of authorized blobs and containers that require anonymous access, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T5 (Very Low) Storage.T50 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C56, depends on Storage.C55, assured by Storage.C59] Ensure anonymous access is set only for required blobs and containers.	Request 1) the mechanism ensuring only required blobs/containers are anonymously accessible, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Medium	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C57, depends on Storage.C55, assured by Storage.C59] Ensure only required blobs and containers are anonymously accessible (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/containers/publicAccess": "Blob"} in Deny mode).	Create or update a non-required blob or a container to be anonymously accessible; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T5 (Medium) Storage.T50 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C59] Verify only required blobs or containers are anonymously accessible (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/containers/publicAccess": "Blob"} in Audit mode).	Create or update a non-required blob or a container to be anonymously accessible; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C81] Verify only the authorized authorization methods are set for authorized blobs, file shares, queues, tables, and DFS (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/protocolSettings.authenticationMethods[*]": ["SharedKey","AzureAD"]} in Audit mode).	Configure a blob, file share, queue, table, or DFS with an unauthorized authorization method; it should be detected.	Medium	Storage.FC3 Storage.FC11	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C90] Maintain a list of storage accounts that require static website hosting.	Request the list of storage accounts that require static website hosting, its review process, and its review records.	Low	Storage.FC2	Storage.T22 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C91, depends on Storage.C90, assured by Storage.C93] Ensure only storage accounts that require static website hosting have it enabled.	Request 1) the mechanism ensuring only required storage accounts have the static website hosting enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T22 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C92, depends on Storage.C90] Prevent storage accounts that do not require static website hosting from having it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/staticWebsite.enabled": true} in Deny mode).	Modify an existing storage account that does not require static website hosting to be enabled; it should be denied.	Medium	Storage.FC2	Storage.T22 (Medium)	Medium

Assurance (COSO) Detect (NIST CSF)	[Storage.C93] Verify storage accounts that do not require static website hosting do not have it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/staticWebsite.enabled": true} in Audit mode).	Modify an existing storage account that does not require static website hosting to be enabled; it should be detected.	Medium	Storage.FC2	-	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C149, depends on Storage.C2, assured by Storage.C81] Ensure required blobs, file shares, queues, tables, and DFS are using authorized authentication methods.	Request 1) the mechanism ensuring blobs, file shares, queues, tables, and DFS use authorized authentication methods, 2) its records of execution for new storage account services, and 3) the plan to move any older storage account services.	Very Low	Storage.FC3 Storage.FC11	Storage.T20 (Medium) Storage.T44 (Medium)	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C161, depends on Storage.C22] Maintain a list of authorized local users, their permissions, and their authentication methods (e.g., password, SSH) for each hierarchical namespace with SFTP enabled.	Request the list of authorized local users, their permissions, their authentication methods, its review process, and its review records.	Low	Storage.FC11	Storage.T44 (Very Low) Storage.T64 (Very Low) Storage.T65 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C162, depends on Storage.C161, assured by Storage.C163] Ensure all local users and associated permissions and authentication methods are authorized.	Request 1) the mechanism ensuring all local users and associated permissions and authentication methods are authorized, 2) its records of execution for all new local users, and 3) the plan to move any older local users.	Low	Storage.FC11	Storage.T64 (Medium) Storage.T65 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C163] Verify all local users and associated permissions and authentication methods are authorized (e.g., by using a custom Azure Policy on "where": {"field": "Microsoft.Storage/storageAccounts/localUsers/permissionScopes[*].permissions", "notIn": "[parameters(\"allowedPermissions\")]"} in Audit mode).	Create a new local user; it should be detected.	Medium	Storage.FC11	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C15] Maintain a list of the blob storage containers that are required to have a minimum retention period enabled.	Request the list of storage account containers that have a minimum retention period according to requirements, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T25 (Very Low) Storage.T39 (Very Low)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C17, depends on Storage.C15] Prevent the creation of required storage accounts without the blob soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/deleteRetentionPolicy.enabled": false} in Deny mode).	Create a required storage account without soft-delete for the blob; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T9 (High) Storage.T25 (Low) Storage.T39 (Very Low)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C20, depends on Storage.C15] Prevent the creation of containers without the soft-delete option enabled (e.g., by using a custom Azure Policy on "Microsoft.Storage/storageAccounts/blobServices/containers/softDelete" in Deny mode).	Create a container without soft-delete; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T9 (High) Storage.T25 (Low) Storage.T39 (Very Low)	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C83] Define the minimum retention period for required file shares (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/deleteRetentionPolicy.days": 7} in Deny mode).	For each file share, request the minimum retention from deletion, its review process, and its review records.	Medium	Storage.FC3	Storage.T18 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C84, depends on Storage.C83, assured by Storage.C86] Ensure file shares have the soft-delete option enabled for at least the defined minimum retention period.	Request 1) the mechanism ensuring file shares have soft-delete enabled for at least the defined minimum retention, 2) its records of execution for all new file	Low	Storage.FC3	Storage.T18 (Medium)	Medium

		shares, and 3) the plan to move any older file shares.				
Preventative (COSO) Protect (NIST CSF)	[Storage.C85, depends on Storage.C83] Prevent the creation of file shares without the soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/shares/deleteRetentionPolicy.enabled": false} in Deny mode).	Create a file share without soft-delete; it should be denied.	Medium	Storage.FC3	Storage.T18 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C86] Verify all file shares have the soft-delete option enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/shares/deleteRetentionPolicy.enabled": false} in Audit mode).	Create a file share without soft-delete; it should be detected.	Medium	Storage.FC3	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C150] Maintain a list of authorized replication policies and their destination storage accounts.	Request the list of authorized replication policies and their destination storage accounts, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T13 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C151, depends on Storage.C150, assured by Storage.C152] Ensure replication policies and their destination storage accounts are authorized.	Request 1) the mechanism ensuring replication policies and their destination storage accounts are authorized, 2) its records of execution for all new replication policies, and 3) the plan to move any older replication policies.	Very Low	Storage.FC1	Storage.T13 (Low)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C152] Verify replication policies and their destination storage accounts are authorized (e.g., by using custom Azure Policy in Audit mode).	Add an unauthorized replication policy; it should be detected.	Medium	Storage.FC1	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C158] Maintain a list of authorized Access Control Lists (ACLs) on Data Lake Storage containers.	Request the list of authorized Access Control Lists (ACLs) on Data Lake Storage containers, its review process, and its review records.	Low	Storage.FC2	Storage.T66 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C159, depends on Storage.C158, assured by Storage.C160] Ensure all Access Control Lists (ACLs) on Data Lake Storage containers are authorized.	Request 1) the mechanism ensuring all Access Control Lists (ACLs) on Data Lake Storage containers are authorized, 2) its records of execution for all new ACLs, and 3) the plan to move any older ACLs.	Low	Storage.FC2	Storage.T66 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C160] Verify all Access Control Lists (ACLs) on Data Lake Storage containers are authorized (e.g., by using a custom Azure Policy on "where": {"field": "Microsoft.Storage/storageAccounts/blobServices/containers/acl[*].id", "notIn": "[parameters (\"authorizedPrincipals\")]"} in Audit mode).	Create a new ACL; it should be detected.	Medium	Storage.FC2	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C98] Maintain a list of file shares that require NFS/SMB 2.1 enabled.	Request the list of file shares that require NFS/SMB 2.1 enabled, its review process, and its review records.	Low	Storage.FC3	Storage.T61 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C99, depends on Storage.C98, assured by Storage.C102] Ensure only file shares that require NFS/SMB 2.1 have it enabled.	Request 1) the mechanism ensuring only file shares that require NFS/SMB 2.1 have it enabled, 2) its records of execution for all new file shares, and 3) the plan to move any older file shares.	Very Low	Storage.FC3	Storage.T61 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C100, depends on Storage.C98] Prevent file shares that do not require NFS/SMB 2.1 from being enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb.protocolVersions[*]": ["SMB2.1"]} in	Modify an existing file share that does not require NFS/SMB 2.1 to use NFS/SMB 2.1; it should be denied.	Medium	Storage.FC3	Storage.T61 (High)	Medium

	Deny mode).					
Assurance (COSO) Detect (NIST CSF)	[Storage.C102] Verify only file shares that require NFS/SMB 2.1 have it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb.protocolVersions[*]": ["SMB2.1"]} in Audit mode).	Modify an existing file share that does not require NFS/SMB 2.1 to use NFS/SMB 2.1; it should be detected.	Medium	Storage.FC3	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C120] Maintain a list of required file shares' security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only).	Request the list of required file share security protocol settings, its review process, and its review records.	Low	Storage.FC3	Storage.T15 (Very Low) Storage.T20 (Very Low) Storage.T60 (Very Low)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C44, depends on Storage.C42] Prevent access from unauthorized IPs by allowing only authorized IPs through the Azure Storage firewall (by using built-in Azure Policy "Storage accounts should restrict network access" in Deny mode).	Access from unauthorized IPs; it should be denied.	Very Low	Storage.FC1 Storage.FC3 Storage.FC4	Storage.T1 (Very Low) Storage.T15 (Medium) Storage.T31 (Medium) Storage.T50 (Medium)	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C60] Maintain a list of authorized customer-managed keys used by storage accounts.	Request the list of authorized customer-managed keys used by storage accounts, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T9 (Very Low) Storage.T38 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C61, depends on Storage.C60, assured by Storage.C65] Ensure only authorized customer-managed keys are configured for storage accounts.	Request 1) the mechanism ensuring only authorized customer-managed keys are used to encrypt each storage account, 2) its records of execution for all new storage accounts, and 3) the plan to move any older authorized storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T9 (Low) Storage.T38 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C63, depends on Storage.C61, assured by Storage.C65] Prevent storage accounts that require customer-managed keys from using service-managed keys (e.g., by using built-in Azure Policy "Storage accounts should use customer-managed key for encryption" in Deny mode).	Create a storage account requiring CMK with a service-managed key; it should be denied.	Medium	Storage.FC1 Storage.FC2	Storage.T9 (Medium) Storage.T38 (High)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C65] Verify only authorized customer-managed keys are configured for storage accounts (e.g., by using the built-in Azure Policy "Storage accounts should use customer-managed key for encryption" in Audit mode).	Modify a required storage account to use an unauthorized CMK; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Medium
Directive (COSO) Identify (NIST CSF)	[Storage.C94] Maintain a list of authorized CORS per endpoint, trusted origins, and corresponding settings.	Request the list of authorized storage accounts with CORS trusted origins and corresponding settings, its review process, and its review records.	Low	Storage.FC1	Storage.T26 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C95, depends on Storage.C94, assured by Storage.C97] Ensure only authorized storage accounts have CORS-trusted origins and corresponding settings configured.	Request 1) the mechanism ensuring only authorized storage accounts have CORS trusted origins and corresponding settings configured, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1	Storage.T26 (Medium)	Medium
Preventative (COSO) Protect (NIST CSF)	[Storage.C96, depends on Storage.C94] Prevent unauthorized storage accounts from using CORS trusted origins and corresponding settings (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/cors.allowedOrigins[*]": ["https://myapp.contoso.com"]} in Deny mode).	Create a storage account with untrusted CORS settings; it should be denied.	Medium	Storage.FC1	Storage.T26 (High)	Medium
Assurance (COSO) Detect (NIST CSF)	[Storage.C97] Verify only authorized CORS trusted origins and	Create a storage account with untrusted CORS settings; it should be detected.	Medium	Storage.FC1	-	Medium

	corresponding settings are configured (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/blobServices/cors.allowedOrigins[*]": ["https://myapp.contoso.com"]} in Audit mode).					
Directive (COSO) Identify (NIST CSF)	[Storage.C22, depends on Storage.C2] Maintain a list of storage accounts that require hierarchical namespace (i.e., Data Lake Storage) and SSH enabled.	Request the list of storage accounts that require hierarchical namespace, its review process, and its review records.	Low	Storage.FC2 Storage.FC11	Storage.T7 (Very Low) Storage.T44 (Very Low) Storage.T64 (Very Low) Storage.T65 (Very Low)	Medium
Directive (COSO) Protect (NIST CSF)	[Storage.C156, depends on Storage.C26, assured by Storage.C157] Ensure all stored access policy permissions are authorized on each container, file share, queue, and table.	Request 1) the mechanism ensuring all stored access policies and their permissions are authorized, 2) its records of execution for all new containers, file shares, queues, and tables, and 3) the plan to move any older containers, file shares, queues, and tables.	Low	Storage.FC4 Storage.FC5	Storage.T27 (Low) Storage.T28 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C157] Verify all stored access policy permissions are authorized (e.g., by using a custom Azure Policy with your allowedPermissions variable set to the permissions you've authorized in Audit mode).	Modify an existing stored access policy's permissions; it should be detected.	Low	Storage.FC4 Storage.FC5	-	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C10, depends on Storage.C144, assured by Storage.C11] Ensure versioning is enabled on required containers.	Request 1) the mechanism ensuring versioning is enabled on required containers, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T7 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C11] Verify versioning is enabled on required containers (e.g., by using Azure built-in policy "Configure your Storage account to enable blob versioning" in Audit mode).	Remove versioning from a container; it should be detected.	Medium	Storage.FC2	-	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C12, depends on Storage.C145, assured by Storage.C13] Ensure snapshots are enabled for required file shares.	Request 1) the mechanism that ensures snapshots are enabled for required file shares, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T7 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C13] Verify snapshots are enabled for required file shares (e.g., by using a custom Azure Policy on {"properties.shareSnapshotEnabled": false} in Audit mode).	Disable snapshotting from a required file share; it should be detected.	Medium	Storage.FC2	-	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C19, depends on Storage.C15, assured by Storage.C21] Ensure required storage accounts have the soft-delete option enabled for the containers.	Request 1) the mechanism ensuring required storage accounts have soft-delete for the container enabled, 2) its records of execution for all new required storage accounts, and 3) the plan to move any older required storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T25 (Low) Storage.T39 (Very Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C21] Verify required storage accounts have container soft delete enabled (e.g., by using custom Azure Policy in Audit mode).	Create a storage account without soft-delete for the container option; it should be detected.	Low	Storage.FC1 Storage.FC2	-	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C46, depends on Storage.C147] Ensure storage blobs are using Azure Backup, following the requirements in the Azure Backup ThreatModel.	Request 1) the mechanism ensuring storage blobs are using Azure Backup, 2) its records of execution for all new storage blobs, and 3) the plan to move any older storage blobs.	High	Storage.FC2	Storage.T7 (Medium) Storage.T9 (Medium) Storage.T12 (Medium)	Low
Directive (COSO)	[Storage.C75]	Request the list of authorized storage account regions	Low	Storage.FC1	Storage.T59 (Very Low)	Low

Identify (NIST CSF)	Maintain a list of authorized storage account regions that can be used for redundancy.	that are used for redundancy, its review process, and its review records.				
Preventative (COSO) Protect (NIST CSF)	[Storage.C77, depends on Storage.C75] Ensure only the authorized storage account region is set for redundancy (e.g., by using a custom Azure Policy on {"location": ["eastus","westeurope"]} in Deny mode).	Create a redundancy configuration on a storage account with an unauthorized region; it should be denied.	Medium	Storage.FC1	Storage.T59 (High)	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C145] Maintain a list of Azure Files that require snapshots.	Request the list of Azure Files that require snapshots, its review process, and its review records.	Low	Storage.FC2	Storage.T7 (Very Low)	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C147] Maintain a list of storage blobs that require Azure Backup.	Request the list of storage blobs that require Azure Backup, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low) Storage.T13 (Very Low)	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C121, depends on Storage.C120, assured by Storage.C123] Ensure required file shares' security protocol settings are set.	Request 1) the mechanism ensuring that the required security protocol settings for file shares in storage accounts are in use, 2) its records of execution for all new file shares, and 3) the plan to move any older file shares.	Low	Storage.FC3	Storage.T15 (Medium) Storage.T20 (Low) Storage.T60 (Medium)	Low
Preventative (COSO) Protect (NIST CSF)	[Storage.C122, depends on Storage.C120] Prevent security protocol settings from changing on required file shares (e.g., by using custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb": {"kerberosTicketEncryption":"AES256","channelEncryption":"Required"}} in Deny mode).	Modify a required file share's security protocol settings; it should be denied.	Medium	Storage.FC3	Storage.T20 (Low) Storage.T60 (High)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C123] Verify required file shares' security protocol settings are configured (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/fileServices/protocolSettings.smb": {"kerberosTicketEncryption":"AES256","channelEncryption":"Required"}} in Audit mode).	Modify a required file share's security protocol settings; it should be detected.	Medium	Storage.FC3	-	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C50] Maintain a list of storage accounts that require diagnostic settings to be enabled and their respective log destinations.	Request the list of storage accounts that require diagnostic settings, its review process, and its review records.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T8 (Very Low) Storage.T9 (Very Low) Storage.T10 (Very Low) Storage.T13 (Very Low) Storage.T42 (Very Low)	Low
Directive (COSO) Protect (NIST CSF)	[Storage.C23, depends on Storage.C22, assured by Storage.C24] Ensure all required storage accounts have hierarchical namespace (i.e., Data Lake Storage) enabled.	Request 1) the mechanism ensuring required storage accounts have hierarchical namespace enabled, 2) its records of execution for all new required storage accounts, 3) the plan to move any older storage accounts with hierarchical namespace.	Low	Storage.FC2	Storage.T7 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C24] Verify only required storage accounts have the hierarchical namespace (HNS) option enabled (e.g., by using a custom Azure Policy on {"isHnsEnabled": "true"} in Audit mode).	Create a non-required storage account with the hierarchical namespace (HNS) option enabled; it should be detected.	Medium	Storage.FC2	-	Low
Directive (COSO) Identify (NIST CSF)	[Storage.C144] Maintain a list of storage account blobs that require versioning and blob change feed to be enabled.	Request the list of storage account blobs that require versioning and blob change feed enabled, along with its	Low	Storage.FC2	Storage.T7 (Very Low)	Low

		review process and review records.				
Directive (COSO) Protect (NIST CSF)	[Storage.C16, depends on Storage.C15, assured by Storage.C18] Ensure required storage accounts have the soft-delete feature for blobs enabled for the defined minimum retention period.	Request 1) the mechanism ensuring required storage accounts have soft-delete for blobs enabled for at least the defined minimum retention, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC2	Storage.T7 (Very Low) Storage.T9 (Very Low) Storage.T12 (Very Low)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C18] Verify required storage accounts have the blob soft-delete option enabled (e.g., by using custom Azure Policy in Audit mode).	Create a required storage account without soft-delete for the blob option; it should be detected.	Medium	Storage.FC2	-	Very Low
Directive (COSO) Identify (NIST CSF)	[Storage.C71] Maintain a list of storage accounts that require redundancy.	Request the list of storage accounts that require redundancy, its review process, and its review records.	Low	Storage.FC3	Storage.T60 (Very Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[Storage.C72, depends on Storage.C71, assured by Storage.C74] Ensure required storage accounts use redundancy.	Request 1) the mechanism ensuring required storage accounts use redundancy, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC3	Storage.T60 (Low)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C74] Verify required storage accounts use redundancy (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/sku.name": ["Standard_GRS","Standard_ZRS"]} in Audit mode).	Remove a redundancy configuration from a storage account; it should be detected.	Medium	Storage.FC3	-	Very Low
Directive (COSO) Protect (NIST CSF)	[Storage.C76, depends on Storage.C75, assured by Storage.C78] Ensure the authorized storage account region used for redundancy is configured.	Request 1) the mechanism ensuring only authorized regions for storage accounts are in use, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1	Storage.T59 (Medium)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C78] Verify only the authorized storage account region is set for redundancy (e.g., by using a custom Azure Policy with {"location": ["eastus","westeurope"]} in Audit mode).	Create a storage account with an unauthorized region; it should be detected.	Medium	Storage.FC1	-	Very Low
Detective (COSO) Detect (NIST CSF)	[Storage.C101] Monitor the creation or update of Azure Files NFS/SMB 2.1 and corresponding settings (e.g., using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly").	Modify or create a file share that does not require NFS/SMB 2.1 to use NFS/SMB 2.1; it should be detected.	Low	Storage.FC3	Storage.T61 (Very Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[Storage.C51, depends on Storage.C50, assured by Storage.C54] Ensure diagnostic settings are enabled on storage accounts that require it, and their respective log destinations are authorized.	Request 1) the mechanism ensuring only authorized diagnostic settings destinations are enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.	Low	Storage.FC1 Storage.FC2	Storage.T7 (Very Low) Storage.T8 (Very Low) Storage.T9 (Very Low) Storage.T10 (Low) Storage.T13 (Very Low) Storage.T42 (Very Low)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C54] Verify storage accounts have diagnostic settings configured (e.g., by using built-in Azure Policy "Configure diagnostic settings for storage accounts to Log Analytics workspace" in Audit mode).	Create a storage account with unauthorized diagnostic settings options; it should be detected.	Medium	Storage.FC1 Storage.FC2	-	Very Low
Directive (COSO) Identify (NIST CSF)	[Storage.C111, depends on Storage.C22] Maintain a list of Data Lake Storage accounts that require SFTP enabled.	Request the list of storage accounts that require SFTP, its review process, and its review records.	Low	Storage.FC11	Storage.T44 (Very Low)	Very Low
Directive (COSO)	[Storage.C114, depends on Storage.C111, assured by Storage.C116] Ensure only storage accounts that require SFTP have it	Request 1) the mechanism ensuring storage accounts	Very Low	Storage.FC11	Storage.T44 (Low)	Very Low

Protect (NIST CSF)	enabled.	that require SFTP have it enabled, 2) its records of execution for all new storage accounts, and 3) the plan to move any older storage accounts.				
Preventative (COSO) Protect (NIST CSF)	[Storage.C115, depends on Storage.C111] Prevent storage accounts that do not require SFTP from having it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/isSftpEnabled": true} in Deny mode).	Modify a storage account that does not require SFTP to use SFTP; it should be denied.	Medium	Storage.FC11	Storage.T44 (Medium)	Very Low
Assurance (COSO) Detect (NIST CSF)	[Storage.C116] Verify only storage accounts that require SFTP have it enabled (e.g., by using a custom Azure Policy on {"Microsoft.Storage/storageAccounts/isSftpEnabled": true} in Audit mode).	Modify a storage account that does not require SFTP to use SFTP; it should be detected.	Medium	Storage.FC11	-	Very Low

Appendix 2 - List of all Actions and their details

Id	Description	Feature Class ID	IAM Permission	Event	API
Storage.A1	Registers the subscription for the storage resource provider and enables the creation of storage accounts.	Storage.FC1	Microsoft.Storage/register/action	Microsoft.Storage/register/action	Providers_Register
Storage.A2	Notifies Azure Storage that virtual network or subnet is being deleted.	Storage.FC1	Microsoft.Storage/locations/deleteVirtualNetworkOrSubnets/action	Microsoft.Storage/locations/deleteVirtualNetworkOrSubnets/action	-
Storage.A3	List blob services of storage account. It returns a collection of one object named default.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/read	-	BlobServices_List
Storage.A4	Retrieves a user delegation key for the blob service. This is only a valid operation when using bearer token authentication.	Storage.FC1	Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action	Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action	Service_GetUserDelegationKey
Storage.A5	Sets the properties of a storage account's blob service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/write	Microsoft.Storage/storageAccounts/blobServices/write	BlobServices_SetServiceProperties
Storage.A6	Gets the properties of a storage account's blob service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/read	-	BlobServices_GetServiceProperties
Storage.A7	Returns a list of the blobs under the specified container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read	-	Blobs_List
Storage.A8	Creates a new block, page, or append blob, or updates the content of an existing block blob. The Put blob operation will overwrite all contents of an existing blob with the same name.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Put_Blob
Storage.A9	Deletes the specified blob or snapshot. Note that in order to delete a blob, you must delete all of its snapshots. You can delete both at the same time with the "Delete blob" operation.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete	Delete_Blob
Storage.A10	Deletes a specific version of a blob without affecting other versions or the current blob.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/deleteblobVersion/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/deleteblobVersion/action	Delete_Blob
Storage.A11	This operation allows for the permanent deletion of soft-deleted blob snapshots or versions before the retention period expires.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/permanentDelete/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/permanentDelete/action	Delete_Blob
Storage.A12	Allows you to create a new blob or overwrite an existing blob within a container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action	Put_Blob
Storage.A13	Allows you to search for blobs within a container based on their assigned tags.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action	Find_BlobsByTags
Storage.A14	Allows you to copy an existing blob to a new location within the same storage account or across different storage accounts.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action	Copy_Blob
Storage.A15	Allows you to set system properties on the blob, such as cache control, content type, and metadata.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/manageOwnership/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/manageOwnership/action	Set_BlobProperties
Storage.A16	Manages access control and permissions for blobs within Azure	Storage.FC2	Microsoft.Storage/storageAccount	Microsoft.Storage/storageAccount	Set_BlobProperties

	Storage.		s/blobServices/containers/blobs/modifyPermissions/action	s/blobServices/containers/blobs/modifyPermissions/action	
Storage.A17	Run as super user.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/runAsSuperUser/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/runAsSuperUser/action	-
Storage.A18	This operation migrates a blob container from container level WORM to object level immutability enabled container. Prerequisites require a container level immutability policy either in locked or unlocked state, account level versioning must be enabled and there should be no legal hold on the container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/migrate/action	Microsoft.Storage/storageAccounts/blobServices/containers/migrate/action	BlobContainers_ObjectLevelWorm
Storage.A19	Updates container properties as specified in request body. Properties not mentioned in the request will be unchanged. Update fails if the specified container doesn't already exist.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/write	Microsoft.Storage/storageAccounts/blobServices/containers/write	BlobContainers_Update
Storage.A20	Deletes specified container under its account.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/delete	Microsoft.Storage/storageAccounts/blobServices/containers/delete	BlobContainers_Delete
Storage.A21	Gets properties of a specified container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/read	-	BlobContainers_Get
Storage.A22	Lists all containers and does not support a prefix like data plane. Also SRP today does not return continuation token.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/read	-	BlobContainers_List
Storage.A23	The Lease container operation establishes and manages a lock on a container for delete operations. The lock duration can be 15 to 60 seconds, or can be infinite.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/lease/action	Microsoft.Storage/storageAccounts/blobServices/containers/lease/action	BlobContainers_Lease
Storage.A24	Creates a new container under the specified account as described by request body. The container resource includes metadata and properties for that container. It does not include a list of the blobs contained by the container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/write	Microsoft.Storage/storageAccounts/blobServices/containers/write	BlobContainers_Create
Storage.A25	Clears legal hold tags. Clearing the same or non-existing tag results in an idempotent operation. ClearLegalHold clears out only the specified tags in the request.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/clearLegalHold/action	Microsoft.Storage/storageAccounts/blobServices/containers/clearLegalHold/action	BlobContainers_ClearLegalHold
Storage.A26	Sets legal hold tags. Setting the same tag results in an idempotent operation. SetLegalHold follows an append pattern and does not clear out the existing tags that are not specified in the request.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/setLegalHold/action	Microsoft.Storage/storageAccounts/blobServices/containers/setLegalHold/action	BlobContainers_SetLegalHold
Storage.A27	Extends the immutabilityPeriodSinceCreationInDays of a locked ImmutabilityPolicy. The only action allowed on a locked policy will be this action. ETag in If-Match is required for this operation.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/extend/action	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/extend/action	BlobContainers_ExtendImmutabilityPolicy
Storage.A28	Aborts an unlocked immutability policy. The response of delete has immutabilityPeriodSinceCreationInDays set to 0. ETag in If-Match is required for this operation. Deleting a locked immutability policy is not allowed, the only way is to delete the container after deleting all expired blobs inside the policy locked container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/delete	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/delete	BlobContainers_DeleteImmutabilityPolicy
Storage.A29	Creates or updates an unlocked immutability policy. ETag in If-Match is honored if given but not required for this operation.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/write	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/write	BlobContainers_CreateOrUpdateImmutabilityPolicy
Storage.A30	Sets the ImmutabilityPolicy to locked state. The only action allowed on a locked policy is ExtendImmutabilityPolicy action. ETag in If-Match is required for this operation.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/lock/action	Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/lock/action	BlobContainers_LockImmutabilityPolicy
Storage.A31	Gets the existing immutability policy along with the corresponding	Storage.FC2	Microsoft.Storage/storageAccount	-	BlobContainers_GetImmutabilityP

	ETag in response Headers and body.		s/blobServices/containers/immutabilityPolicies/read		olicy
Storage.A32	List all queue services for the storage account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/read	-	QueueServices_List
Storage.A33	Gets the properties of a storage account's queue service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/read	-	QueueServices_GetServiceProperties
Storage.A34	Sets the properties of a storage account's queue service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/write	Microsoft.Storage/storageAccounts/queueServices/write	QueueServices_SetServiceProperties
Storage.A35	Creates a new queue with the specified queue name, under the specified account. Creates a new queue with the specified queue name, under the specified account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/write	Microsoft.Storage/storageAccounts/queueServices/queues/write	Queue_Create Queue_Update
Storage.A36	Gets the queue with the specified queue name, under the specified account if it exists. Gets a list of all the queues under the specified storage account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/read	-	Queue_Get Queue_List
Storage.A37	Creates a new queue with the specified queue name, under the specified account. Creates a new queue with the specified queue name, under the specified account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/write	Microsoft.Storage/storageAccounts/queueServices/queues/write	Queue_Create Queue_Update
Storage.A38	Deletes the queue with the specified queue name, under the specified account if it exists.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/delete	Microsoft.Storage/storageAccounts/queueServices/queues/delete	Queue_Delete
Storage.A39	Retrieves one or more messages from the front of the queue.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/messages/read	-	Get_Messages
Storage.A40	Adds a new message to the back of the message queue. A visibility time-out can also be specified to make the message invisible until the visibility time-out expires. A message must be in a format that can be included in an XML request with UTF-8 encoding. The encoded message can be up to 64 kibibytes (KiB) in size for version 2011-08-18 and later, or 8 KiB for earlier versions.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/messages/write	Microsoft.Storage/storageAccounts/queueServices/queues/messages/write	Put_Messages
Storage.A41	Deletes the specified message from the queue.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/messages/delete	Microsoft.Storage/storageAccounts/queueServices/queues/messages/delete	Delete_Messages
Storage.A42	This operation allows you to add a new message to the back of a specified queue.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/messages/add/action	Microsoft.Storage/storageAccounts/queueServices/queues/messages/add/action	Put_Messages
Storage.A43	Handles operations that involve processing messages in Azure Queue Storage. This encompasses actions such as retrieving messages from a queue, updating their visibility, and deleting them after processing.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/messages/process/action	Microsoft.Storage/storageAccounts/queueServices/queues/messages/process/action	-
Storage.A44	The update operation can be used to update the SKU, encryption, access tier, or tags for a storage account. It can also be used to map the account to a custom domain. Only one custom domain is supported per storage account; the replacement/change of custom domain is not supported.	Storage.FC1	Microsoft.Storage/storageAccounts/updateInternalProperties/action	Microsoft.Storage/storageAccounts/updateInternalProperties/action	StorageAccounts_Update
Storage.A45	Live migration of storage account to enable HNS.	Storage.FC1	Microsoft.Storage/storageAccounts/hnsonmigration/action	Microsoft.Storage/storageAccounts/hnsonmigration/action	StorageAccounts_HierarchicalNamespaceMigration
Storage.A46	Live migration of storage account to enable HNS.	Storage.FC1	Microsoft.Storage/storageAccount	Microsoft.Storage/storageAccount	StorageAccounts_HierarchicalNa

			s/hnsonmigration/action	s/hnsonmigration/action	mespaceMigration
Storage.A47	Restore blobs in the specified blob ranges.	Storage.FC2	Microsoft.Storage/storageAccounts/restoreBlobRanges/action	Microsoft.Storage/storageAccounts/restoreBlobRanges/action	StorageAccounts_RestoreBlobRanges
Storage.A48	Used for approving or rejecting private endpoint connections for Azure Storage accounts.	Storage.FC12	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	PrivateEndpointConnections_Put
Storage.A49	A failover request can be triggered for a storage account in the event a primary endpoint becomes unavailable for any reason. The failover occurs from the storage account's primary cluster to the secondary cluster for RA-GRS accounts. The secondary cluster will become primary after failover and the account is converted to LRS. In the case of a Planned failover, the primary and secondary clusters are swapped after failover and the account remains geo-replicated. Failover should continue to be used in the event of availability issues as Planned failover is only available while the primary and secondary endpoints are available. The primary use case of a Planned failover is Disaster Recovery testing drills. This type of failover is invoked by setting failoverType parameter to 'Planned'. Learn more about the failover options here- "https://learn.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance".	Storage.FC1	Microsoft.Storage/storageAccounts/failover/action	Microsoft.Storage/storageAccounts/failover/action	StorageAccounts_Failover
Storage.A50	Lists the access keys or Kerberos keys (if Active Directory enabled) for the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/listKeys/action	Microsoft.Storage/storageAccounts/listKeys/action	StorageAccounts_ListKeys
Storage.A51	Regenerates one of the access keys or Kerberos keys for the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/regenerateKey/action	Microsoft.Storage/storageAccounts/regenerateKey/action	StorageAccounts_RegenerateKey
Storage.A52	Used as part of the regenerate keys process.	Storage.FC1	Microsoft.Storage/storageAccounts/rotateKey/action	Microsoft.Storage/storageAccounts/rotateKey/action	StorageAccounts_RegenerateKey
Storage.A53	Revoke user delegation keys.	Storage.FC1	Microsoft.Storage/storageAccounts/revokeUserDelegationKeys/action	Microsoft.Storage/storageAccounts/revokeUserDelegationKeys/action	StorageAccounts_RevokeUserDelegationKeys
Storage.A54	Deletes a storage account in Microsoft Azure.	Storage.FC1	Microsoft.Storage/storageAccounts/delete	Microsoft.Storage/storageAccounts/delete	StorageAccounts_Delete
Storage.A55	Lists all the storage accounts available under the subscription.	Storage.FC1	Microsoft.Storage/storageAccounts/read	-	StorageAccounts_List
Storage.A56	List SAS credentials of a storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/ListAccountSas/action	Microsoft.Storage/storageAccounts/ListAccountSas/action	StorageAccounts_ListAccountSAS
Storage.A57	List service SAS credentials of a specific resource.	Storage.FC1	Microsoft.Storage/storageAccounts/ListServiceSas/action	Microsoft.Storage/storageAccounts/ListServiceSas/action	StorageAccounts_ListServiceSAS
Storage.A58	Asynchronously creates a new storage account with the specified parameters. If an account is already created and a subsequent create request is issued with different properties, the account properties will be updated. If an account is already created and a subsequent create or update request is issued with the exact same set of properties, the request will succeed. The update operation can be used to update the SKU, encryption, access tier, or tags for a storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/write	Microsoft.Storage/storageAccounts/write	StorageAccounts_Create
Storage.A59	Configure monitoring and logging settings through Azure Resource Manager (ARM) APIs.	Storage.FC1	Microsoft.Storage/storageAccounts/services/diagnosticsettings/write	Microsoft.Storage/storageAccounts/services/diagnosticsettings/write	StorageAccounts_CreateOrUpdateDiagnosticSettings

Storage.A79	Lists the available SKUs supported by Microsoft.Storage for given subscription.	Storage.FC1	Microsoft.Storage/skus/read	-	Skus_List
Storage.A80	Lists all of the available storage REST API operations.	Storage.FC1	Microsoft.Storage/operations/read	-	Operations_List
Storage.A81	Checks that the storage account name is valid and is not already in use.	Storage.FC1	Microsoft.Storage/checkNameAvailability/read	-	StorageAccounts_CheckNameAvailability
Storage.A82	Gets the current usage count and the limit for the resources of the location under the subscription.	Storage.FC1	Microsoft.Storage/locations/usages/readMicrosoft.Storage/locations/usages/read	-	Usages_ListByLocation
Storage.A83	Gets the current usage count and the limit for the resources under the subscription.	Storage.FC1	Microsoft.Storage/usages/read	-	Usage_List
Storage.A84	The get tags operation enables users to get the tags associated with a blob.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/read	-	Blob_GetTags
Storage.A85	The set tags operation enables users to set the tags associated with a blob.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write	Blob_SetTags
Storage.A86	Deletes the managementpolicy associated with the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/managementPolicies/delete	Microsoft.Storage/storageAccounts/managementPolicies/delete	ManagementPolicies_Delete
Storage.A87	Gets the managementpolicy associated with the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/managementPolicies/read	-	ManagementPolicies_Get
Storage.A88	Sets the managementpolicy to the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/managementPolicies/write	Microsoft.Storage/storageAccounts/managementPolicies/write	ManagementPolicies_CreateOrUpdate
Storage.A89	Used for operations that manage Azure file shares within a storage account.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/action	Microsoft.Storage/storageAccounts/fileServices/shares/action	-
Storage.A90	List all file services in storage accounts.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/read	-	FileServices_List
Storage.A91	Sets the properties of file services in storage accounts, including CORS (Cross-Origin Resource Sharing) rules.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/write	Microsoft.Storage/storageAccounts/fileServices/write	FileServices_SetServiceProperties
Storage.A92	Gets the properties of file services in storage accounts, including CORS (Cross-Origin Resource Sharing) rules.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/read	-	FileServices_GetServiceProperties
Storage.A93	List all table services for the storage account.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/read	-	TableServices_List
Storage.A94	Gets the properties of a storage account's table service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/read	-	TableServices_GetServiceProperties
Storage.A95	Sets the properties of a storage account's table service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/write	Microsoft.Storage/storageAccounts/tableServices/write	TableServices_SetServiceProperties
Storage.A96	Reads or downloads a file from the system, including its metadata and properties.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/read	-	Get_File
Storage.A97	Creates a new file or replaces a file. When you call "Create File", you only initialize the file. To add content to a file, you call the "Put Range" operation.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write	Create_File
Storage.A98	The Delete file operation immediately removes the file from the storage account.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/delete	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/delete	Delete_File

Storage.A99	The Set file properties operation sets system properties on the file.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/modifyPermissions/action	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/modifyPermissions/action	Set_FileProperties
Storage.A100	The Get file properties operation returns all user-defined metadata, standard HTTP properties, and system properties for the file. It doesn't return the content of the file.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/actassuperuser/action	Microsoft.Storage/storageAccounts/fileServices/fileshares/files/actassuperuser/action	Get_FileProperties
Storage.A101	Get a private endpoint connection proxy.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/read	-	PrivateEndpointConnectionProxies_Get
Storage.A102	Delete private endpoint connection proxies.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/delete	Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/delete	PrivateEndpointConnectionProxies_Delete
Storage.A103	List all private endpoint connection proxies.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/write	Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/write	PrivateEndpointConnectionProxies_List
Storage.A104	List all the private endpoint connections associated with the storage account.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	-	PrivateEndpointConnections_List
Storage.A105	Deletes the specified private endpoint connection associated with the storage account.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnections/delete	Microsoft.Storage/storageAccounts/privateEndpointConnections/delete	PrivateEndpointConnections_Delete
Storage.A106	Gets the specified private endpoint connection associated with the storage account.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	-	PrivateEndpointConnections_Get
Storage.A107	Update the state of specified private endpoint connection associated with the storage account.	Storage.FC12	Microsoft.Storage/storageAccounts/privateEndpointConnections/write	Microsoft.Storage/storageAccounts/privateEndpointConnections/write	PrivateEndpointConnections_Put
Storage.A108	Gets the Private Link resources that need to be created for a storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/privateLinkResources/read	-	PrivateLinkResources_ListByStorageAccount
Storage.A109	Checks that the storage account name is valid and is not already in use.	Storage.FC1	Microsoft.Storage/locations/checkNameAvailability/read	-	StorageAccounts_CheckNameAvailability
Storage.A110	Deletes specified share under its account.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/delete	Microsoft.Storage/storageAccounts/fileServices/shares/delete	FileShares_Delete
Storage.A111	Lists all shares. Gets properties of a specified share.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/read	-	FileShares_List FileShares_Get
Storage.A112	Lists all shares. Gets properties of a specified share.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/read	-	FileShares_List FileShares_Get
Storage.A113	Creates a new share under the specified account as described by request body. The share resource includes metadata and properties for that share. It does not include a list of the files contained by the share. Updates share properties as specified in request body. Properties not mentioned in the request will not be changed. Update fails if the specified share does not already exist.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/write	Microsoft.Storage/storageAccounts/fileServices/shares/write	FileShares_Create
Storage.A114	Returns the properties for the specified encryption scope.	Storage.FC1	Microsoft.Storage/storageAccounts/encryptionScopes/read	-	EncryptionScopes_Get
Storage.A115	Synchronously creates or updates an encryption scope under the specified storage account. If an encryption scope is already	Storage.FC1	Microsoft.Storage/storageAccounts/encryptionScopes/write	Microsoft.Storage/storageAccounts/encryptionScopes/write	EncryptionScopes_Put

	created and a subsequent request is issued with different properties, the encryption scope properties will be updated per the specified request. Update encryption scope properties as specified in the request body. Update fails if the specified encryption scope does not already exist.				
Storage.A120	Removes a data share policy.	Storage.FC1	Microsoft.Storage/storageAccounts/dataSharePolicies/delete	Microsoft.Storage/storageAccounts/dataSharePolicies/delete	Delete_DataSharePolicy
Storage.A121	Gets a data share policy for a specific account.	Storage.FC1	Microsoft.Storage/storageAccounts/dataSharePolicies/read	-	Get_DataSharePolicy
Storage.A122	Crates or updates a data share policy.	Storage.FC1	Microsoft.Storage/storageAccounts/dataSharePolicies/write	Microsoft.Storage/storageAccounts/dataSharePolicies/write	CreateOrUpdate_DataSharePolicy
Storage.A123	Deletes the local user associated with the specified storage account.	Storage.FC11	Microsoft.Storage/storageAccounts/localUsers/delete	Microsoft.Storage/storageAccounts/localUsers/delete	LocalUsers_Delete
Storage.A124	Regenerate the local user SSH password.	Storage.FC11	Microsoft.Storage/storageAccounts/localUsers/regeneratePassword/action	Microsoft.Storage/storageAccounts/localUsers/regeneratePassword/action	LocalUsers_RegeneratePassword
Storage.A125	List SSH authorized keys and Shared Key of the local user.	Storage.FC11	Microsoft.Storage/storageAccounts/localUsers/listKeys/action	Microsoft.Storage/storageAccounts/localUsers/listKeys/action	LocalUsers_ListKeys
Storage.A126	List the local users associated with the storage account.	Storage.FC11	Microsoft.Storage/storageAccounts/localUsers/read	-	LocalUsers_List
Storage.A127	Get the local user of the storage account by username.	Storage.FC11	Microsoft.Storage/storageAccounts/localUsers/read	-	LocalUsers_Get
Storage.A128	Create or update the properties of a local user associated with the storage account. Properties for NFSv3 enablement and extended Groups cannot be set with other properties.	Storage.FC11	Microsoft.Storage/storageAccounts/localUsers/write	Microsoft.Storage/storageAccounts/localUsers/write	LocalUsers_CreateOrUpdate
Storage.A129	Gets the table with the specified table name, under the specified account if it exists. Gets a list of all the tables under the specified storage account.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/read	-	Table_Get Table_List
Storage.A130	Creates a new table with the specified table name, under the specified account. Creates a new table with the specified table name, under the specified account.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/write	Microsoft.Storage/storageAccounts/tableServices/tables/write	Table_Create Table_Update
Storage.A131	Deletes the table with the specified table name, under the specified account if it exists.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/delete	Microsoft.Storage/storageAccounts/tableServices/tables/delete	Table_Delete
Storage.A132	Deletes the blob inventory policy associated with the specified storage account.	Storage.FC10	Microsoft.Storage/storageAccounts/inventoryPolicies/delete	Microsoft.Storage/storageAccounts/inventoryPolicies/delete	BlobInventoryPolicies_Delete
Storage.A133	Gets the blob inventory policy associated with the specified storage account.	Storage.FC10	Microsoft.Storage/storageAccounts/inventoryPolicies/read	-	BlobInventoryPolicies_Get
Storage.A134	Sets the blob inventory policy to the specified storage account.	Storage.FC10	Microsoft.Storage/storageAccounts/inventoryPolicies/write	Microsoft.Storage/storageAccounts/inventoryPolicies/write	BlobInventoryPolicies_CreateOrUpdate
Storage.A135	Part of the Azure Management resource lock.	Storage.FC1	Microsoft.Storage/storageAccounts/accountLocks/deleteLock/action	Microsoft.Storage/storageAccounts/accountLocks/deleteLock/action	-
Storage.A136	Lock read.	Storage.FC1	Microsoft.Storage/storageAccounts/accountLocks/read	-	ManagementLock_List
Storage.A137	Lock write.	Storage.FC1	Microsoft.Storage/storageAccounts/accountLocks/write	Microsoft.Storage/storageAccounts/accountLocks/write	ManagementLock_CreateOrUpdate
Storage.A138	Lock delete.	Storage.FC1	Microsoft.Storage/storageAccount	Microsoft.Storage/storageAccount	ManagementLock_Delete

			s/accountLocks/delete	s/accountLocks/delete	
Storage.A139	Data share policy read.	Storage.FC1	Microsoft.Storage/storageAccounts/consumerdataSharePolicies/read	-	-
Storage.A140	Data share policy write.	Storage.FC1	Microsoft.Storage/storageAccounts/consumerdataSharePolicies/write	Microsoft.Storage/storageAccounts/consumerdataSharePolicies/write	-
Storage.A141	Query table entities.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/entities/read	-	-
Storage.A142	Insert, merge, or replace table entities.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/entities/write	Microsoft.Storage/storageAccounts/tableServices/tables/entities/write	-
Storage.A143	Delete table entities.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/entities/delete	Microsoft.Storage/storageAccounts/tableServices/tables/entities/delete	-
Storage.A144	Insert table entities.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/entities/add/action	Microsoft.Storage/storageAccounts/tableServices/tables/entities/add/action	-
Storage.A145	Merge or update table entities.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/entities/update/action	Microsoft.Storage/storageAccounts/tableServices/tables/entities/update/action	-
Storage.A146	Run as super user.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/immutableStorage/runAsSuperUser/action	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/immutableStorage/runAsSuperUser/action	-
Storage.A147	Create object replication restore point marker.	Storage.FC1	Microsoft.Storage/storageAccounts/objectReplicationPolicies/restorePointMarkers/write	Microsoft.Storage/storageAccounts/objectReplicationPolicies/restorePointMarkers/write	-
Storage.A148	Delete object replication restore point.	Storage.FC1	Microsoft.Storage/storageAccounts/restorePoints/delete	Microsoft.Storage/storageAccounts/restorePoints/delete	-
Storage.A149	List object replication restore points.	Storage.FC1	Microsoft.Storage/storageAccounts/restorePoints/read	-	-
Storage.A150	List object replication restore points.	Storage.FC1	Microsoft.Storage/storageAccounts/restorePoints/read	-	-
Storage.A151	Gets the status of the ongoing migration for the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/accountMigrations/read	-	StorageAccounts_GetCustomerInitiatedMigration
Storage.A152	Customer is able to update their storage account redundancy for increased resiliency.	Storage.FC1	Microsoft.Storage/storageAccounts/accountMigrations/write	Microsoft.Storage/storageAccounts/accountMigrations/write	-
Storage.A153	Lists all containers and does not support a prefix like data plane. Also SRP today does not return continuation token. Gets properties of a specified container.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/read	-	BlobContainers_List
Storage.A154	Creates a new container under the specified account. If the container with the same name already exists, the operation fails returns all user-defined metadata and system properties for the specified container. The data returned does not include the container's list of blobs operation marks the specified container for	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/write	Microsoft.Storage/storageAccounts/blobServices/containers/write	Container_Create

	deletion. The container and any blobs contained within it are later deleted during garbage collection restype.				
Storage.A155	Set properties for the filesystem. This operation supports conditional HTTP requests. For more information, see [Specifying conditional Headers for blob service operations](https://docs.microsoft.com/en-us/rest/API/storageservices/specifying-conditional-headers-for-blob-service-operations).	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	FileSystem_SetProperties
Storage.A156	List filesystem paths and their properties.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read	-	FileSystem_ListPaths
Storage.A157	List blob services of storage account. It returns a collection of one object named default. Gets the properties of a storage account's blob service, including properties for storage Analytics and CORS (Cross-Origin Resource Sharing) rules.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/read	-	BlobServices_GetServiceProperties
Storage.A158	Deletes specified container under its account.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/delete	Microsoft.Storage/storageAccounts/blobServices/containers/delete	BlobContainers_Delete
Storage.A159	Create or rename a file or directory. By default, the destination is overwritten and if the destination already exists and has a lease the lease is broken. This operation supports conditional HTTP requests. For more information, see [Specifying conditional Headers for blob service operations](https://docs.microsoft.com/en-us/rest/API/storageservices/specifying-conditional-headers-for-blob-service-operations). To fail if the destination already exists, use a conditional request with If-None-Match: "*".	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Path_Create
Storage.A160	Uploads data to be appended to a file, flushes (writes) previously uploaded data to a file, sets properties for a file or directory, or sets access control for a file or directory. Data can only be appended to a file. Concurrent writes to the same file using multiple clients are not supported. This operation supports conditional HTTP requests. For more information, see [Specifying conditional Headers for blob service operations](https://docs.microsoft.com/en-us/rest/API/storageservices/specifying-conditional-headers-for-blob-service-operations).	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Path_Update
Storage.A161	The Lease container operation establishes and manages a lock on a container for delete operations. The lock duration can be 15 to 60 seconds, or can be infinite.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/lease/action	Microsoft.Storage/storageAccounts/blobServices/containers/lease/action	BlobContainers_Lease
Storage.A162	The "Download" operation reads or downloads a blob from the system, including its metadata and properties. You can also call "Download" to read a snapshot.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read	-	Blob_Download
Storage.A163	The Get properties operation returns all user-defined metadata, standard HTTP properties, and system properties for the blob. It does not return the content of the blob.	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read	-	Blob_GetProperties
Storage.A164	If the storage account's soft delete feature is disabled then, when a blob is deleted, it is permanently removed from the storage account. If the storage account's soft delete feature is enabled, then, when a blob is deleted, it is marked for deletion and becomes inaccessible immediately. However, the blob service	Storage.FC2	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete	Blob_Delete

	retains the blob or snapshot for the number of days specified by the DeleteRetentionPolicy section of [storage service properties] (Set-Blob-Service-Properties.md). After the specified number of days has passed, the blob's data is permanently removed from the storage account. Note that you continue to be charged for the soft-deleted blob's storage until it is permanently removed. Use the "List Blobs" API and specify the "include=deleted" query parameter to discover which blobs and snapshots have been soft deleted. You can then use the Undelete blob API to restore a soft-deleted blob. All other operations on a soft-deleted blob or snapshot causes the service to return an HTTP status code of 404 (ResourceNotFound).				
Storage.A165	Gets the current usage count and the limit for the resources under the subscription.	Storage.FC1	Microsoft.Storage/usages/read	-	Usage_List
Storage.A166	Lists all shares.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/read	-	FileShares_List
Storage.A167	Updates share properties as specified in request body. Properties not mentioned in the request will not be changed. Update fails if the specified share does not already exist.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/write	Microsoft.Storage/storageAccounts/fileServices/shares/write	FileShares_Update
Storage.A168	Gets properties of a specified share.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/read	-	FileShares_Get
Storage.A169	Restore a file share within a valid retention days if share soft delete is enabled.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/restore/action	Microsoft.Storage/storageAccounts/fileServices/shares/restore/action	FileShares_Restore
Storage.A170	The "Lease Share" operation establishes and manages a lock on a share for delete operations. The lock duration can be 15 to 60 seconds, or can be infinite.	Storage.FC3	Microsoft.Storage/storageAccounts/fileServices/shares/lease/action	Microsoft.Storage/storageAccounts/fileServices/shares/lease/action	FileShares_Lease
Storage.A171	Gets list of effective NetworkSecurityPerimeterConfiguration for storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/networkSecurityPerimeterConfigurations/read	-	NetworkSecurityPerimeterConfigurations_List
Storage.A172	Gets effective NetworkSecurityPerimeterConfiguration for association.	Storage.FC1	Microsoft.Storage/storageAccounts/networkSecurityPerimeterConfigurations/read	-	NetworkSecurityPerimeterConfigurations_Get
Storage.A173	Refreshes any information about the association.	Storage.FC1	Microsoft.Storage/storageAccounts/networkSecurityPerimeterConfigurations/reconcile/action	Microsoft.Storage/storageAccounts/networkSecurityPerimeterConfigurations/reconcile/action	NetworkSecurityPerimeterConfigurations_Reconcile
Storage.A174	Gets the queue with the specified queue name, under the specified account if it exists.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/read	-	Queue_Get
Storage.A175	Gets a list of all the queues under the specified storage account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/read	-	Queue_List
Storage.A176	Creates a new queue with the specified queue name, under the specified account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/write	Microsoft.Storage/storageAccounts/queueServices/queues/write	Queue_Create
Storage.A177	Creates a new queue with the specified queue name, under the specified account.	Storage.FC4	Microsoft.Storage/storageAccounts/queueServices/queues/write	Microsoft.Storage/storageAccounts/queueServices/queues/write	Queue_Update
Storage.A178	Lists deleted accounts under the subscription.	Storage.FC1	Microsoft.Storage/deletedAccounts/read	-	DeletedAccounts_List
Storage.A179	Get properties of specified deleted account resource.	Storage.FC1	Microsoft.Storage/locations/deletedAccounts/read	-	DeletedAccounts_Get

Storage.A180	Gets the current usage count and the limit for the resources of the location under the subscription.	Storage.FC1	Microsoft.Storage/locations/usages/read	-	Usage_ListByLocation
Storage.A181	Lists all the storage accounts available under the given resource group. Note that storage keys are not returned; use the ListKeys operation for this.	Storage.FC1	Microsoft.Storage/storageAccounts/read	-	StorageAccounts_ListByResourceGroup
Storage.A182	Returns the properties for the specified storage account including but not limited to name, SKU name, location, and account status. The ListKeys operation should be used to retrieve storage keys.	Storage.FC1	Microsoft.Storage/storageAccounts/read	-	StorageAccounts_GetProperties
Storage.A183	Lists all the encryption scopes available under the specified storage account.	Storage.FC1	Microsoft.Storage/storageAccounts/encryptionScopes/read	-	EncryptionScopes_List
Storage.A184	Update encryption scope properties as specified in the request body. Update fails if the specified encryption scope does not already exist.	Storage.FC1	Microsoft.Storage/storageAccounts/encryptionScopes/write	Microsoft.Storage/storageAccounts/encryptionScopes/write	EncryptionScopes_Patch
Storage.A185	Gets the blob inventory policy associated with the specified storage account.	Storage.FC10	Microsoft.Storage/storageAccounts/inventoryPolicies/read	-	BlobInventoryPolicies_List
Storage.A186	Abort live migration of storage account to enable HNS.	Storage.FC1	Microsoft.Storage/storageAccounts/aborthnsonmigration/action	Microsoft.Storage/storageAccounts/aborthnsonmigration/action	StorageAccounts_AbortHierarchicalNamespaceMigration
Storage.A187	Account migration request can be triggered for a storage account to change its redundancy level. The migration updates the non-zonal redundant storage account to a zonal redundant account or vice-versa in order to have better reliability and availability. Zone-redundant storage (ZRS) replicates your storage account synchronously across three Azure Availability Zones in the primary region.	Storage.FC1	Microsoft.Storage/storageAccounts/startAccountMigration/action	Microsoft.Storage/storageAccounts/startAccountMigration/action	StorageAccounts_CustomerInitiatedMigration
Storage.A188	List all the storage task assignments in an account.	Storage.FC1	Microsoft.Storage/storageAccounts/storageTaskAssignments/read	-	StorageTaskAssignments_List
Storage.A189	Get the storage task assignment properties.	Storage.FC1	Microsoft.Storage/storageAccounts/storageTaskAssignments/read	-	StorageTaskAssignments_Get
Storage.A190	Asynchronously creates a new storage task assignment sub-resource with the specified parameters. If a storage task assignment is already created and a subsequent create request is issued with different properties, the storage task assignment properties will be updated. If a storage task assignment is already created and a subsequent create or update request is issued with the exact same set of properties, the request will succeed.	Storage.FC1	Microsoft.Storage/storageAccounts/storageTaskAssignments/write	Microsoft.Storage/storageAccounts/storageTaskAssignments/write	StorageTaskAssignments_Create
Storage.A191	Update storage task assignment properties.	Storage.FC1	Microsoft.Storage/storageAccounts/storageTaskAssignments/write	Microsoft.Storage/storageAccounts/storageTaskAssignments/write	StorageTaskAssignments_Update
Storage.A192	Delete the storage task assignment sub-resource.	Storage.FC1	Microsoft.Storage/storageAccounts/storageTaskAssignments/delete	Microsoft.Storage/storageAccounts/storageTaskAssignments/delete	StorageTaskAssignments_Delete
Storage.A193	Fetch the report summary of all the storage task assignments and instances in an account.	Storage.FC1	Microsoft.Storage/storageAccounts/reports/read	-	StorageTaskAssignmentsInstancesReport_List
Storage.A194	Fetch the report summary of a single storage task assignment's instances.	Storage.FC1	Microsoft.Storage/storageAccounts/storageTaskAssignments/reports/read	-	StorageTaskAssignmentInstancesReport_List
Storage.A195	Gets a list of all the tables under the specified storage account.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/read	-	Table_List
Storage.A196	Gets the table with the specified table name, under the specified	Storage.FC5	Microsoft.Storage/storageAccount	-	Table_Get

	account if it exists.		s/tableServices/tables/read		
Storage.A197	Creates a new table with the specified table name, under the specified account.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/write	Microsoft.Storage/storageAccounts/tableServices/tables/write	Table_Create
Storage.A198	Creates a new table with the specified table name, under the specified account.	Storage.FC5	Microsoft.Storage/storageAccounts/tableServices/tables/write	Microsoft.Storage/storageAccounts/tableServices/tables/write	Table_Update
Storage.A199	A failover request can be triggered for a storage account in the event a primary endpoint becomes unavailable for any reason. The failover occurs from the storage account's primary cluster to the secondary cluster for RA-GRS accounts. The secondary cluster will become primary after failover and the account is converted to LRS. In the case of a Planned failover, the primary and secondary clusters are swapped after failover and the account remains geo-replicated. Failover should continue to be used in the event of availability issues as Planned failover is only available while the primary and secondary endpoints are available. The primary use case of a Planned failover is Disaster Recovery testing drills. This type of failover is invoked by setting "FailoverType" parameter to 'Planned'. Learn more about the failover options here ref.	Storage.FC1	Microsoft.Storage/storageAccounts/failover/action	Microsoft.Storage/storageAccounts/failover/action	StorageAccounts_Failover
Storage.A200	Delete a storage connector.	Storage.FC1	Microsoft.Storage/storageAccounts/connectors/delete	-	-
Storage.A201	Returns the list of storage connectors or gets the properties of specified storage connector.	Storage.FC1	Microsoft.Storage/storageAccounts/connectors/read	-	-
Storage.A202	Test the connection of an existing storage connector.	Storage.FC1	Microsoft.Storage/storageAccounts/connectors/testExistingConnection/action	-	-
Storage.A203	Creates or updates a storage connector.	Storage.FC1	Microsoft.Storage/storageAccounts/connectors/write	-	-
Storage.A204	Delete a storage data share.	Storage.FC1	Microsoft.Storage/storageAccounts/dataShares/delete	-	-
Storage.A205	Returns the list of storage data shares or gets the properties of specified storage data share.	Storage.FC1	Microsoft.Storage/storageAccounts/dataShares/read	-	-
Storage.A206	Creates or updates a storage data share.	Storage.FC1	Microsoft.Storage/storageAccounts/dataShares/write	-	-
Storage.A207	Revert file share.	Storage.FC1	Microsoft.Storage/storageAccounts/fileServices/shares/revert/action	-	-