# ThreatModel for Azure Storage

### Introduction

Read the blog: TBD

### 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

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/). This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.



### Source

The latest version of this work is hosted on [GitHub](https://github.com/trustoncloud/threatmodel-for-azure-storage).

### Contact

If you have any questions, please contact [chatbot@trustoncloud.com](mailto:chatbot@trustoncloud.com).

| **Azure Storage** Data Flow Diagram | Security Scorecard  | ***Security in the Cloud*** | | | --- | --- | | Number of Actions\* | 164 | | Identity management | Azure IAM | | Number of IAM permissions\* | 139 | | Resource-based access | DFS ACL, file share ACL,  queue ACL, table ACL,  storage account access keys,  SAS tokens | | Logging Coverage for APIs | 100.0% | | Number of Logging Event Names\* | 164 | | Network Filtering | VNET security,  Storage Account Firewall | | Encryption-at-rest | Yes | | Encryption-in-transit | Yes |   \* See details in Appendixes |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

## Mitre ATT&CK matrix for Azure Storage

| **Initial Access** | **Execution** | **Persistence** | **Privilege Escalation** | **Defense Evasion** | **Credential Access** | **Discovery** | **Lateral Movement** | **Collection** | **Exfiltration** | **Impact** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Infect with malware downstream processes [Storage.T12] | Privilege escalation by modifying file system ACL [Storage.T6] |  |  |  |  |  | Privilege escalation accessing storage access key [Storage.T1] | Block data access of a SAS token [Storage.T2] |
|  |  | Distribute malicious files via file share [Storage.T20] | Privilege escalation by modifying file share ACL [Storage.T17] |  |  |  |  |  | Exfiltrate data using account key access or SAS token [Storage.T3] | Recursively delete DFS directories and their content [Storage.T7] |
|  |  | Distribute malicious infected files via a reputed web address [Storage.T22] | Usage outdated protocols to access file shares [Storage.T21] |  |  |  |  |  | Use storage account name to steal data or distribute malicious data [Storage.T4] | Unauthorised modification of data [Storage.T8] |
|  |  |  | Unauthorized data exposed by breaking CORS settings [Storage.T26] |  |  |  |  |  | Unauthorized data made public [Storage.T5] | Files encrypted by ransomware in DFS/blob [Storage.T9] |
|  |  |  | Privilege escalation by modifying queue ACL [Storage.T27] |  |  |  |  |  | Exfiltrate data using diagnostic settings [Storage.T10] | Increase billing by file share overflow [Storage.T16] |
|  |  |  | Privilege escalation by modifying table ACL [Storage.T28] |  |  |  |  |  | Man-in-the-middle attack via any storage account endpoint [Storage.T11] | Recursively delete directories and the content in the file share [Storage.T18] |
|  |  |  |  |  |  |  |  |  | Unauthorised access to data via storage account replication [Storage.T13] | Files encrypted by ransomware in file shares [Storage.T19] |
|  |  |  |  |  |  |  |  |  | Unauthorised access to data by direct access to the physical disk [Storage.T14] | Recursively delete data using blob storage lifecycle management [Storage.T25] |
|  |  |  |  |  |  |  |  |  | Exfiltrate data using different access method [Storage.T15] | DDoS on endpoint [Storage.T29] |
|  |  |  |  |  |  |  |  |  | Exfiltrate data using different service [Storage.T23] | Impacting queues messages integrity or complete data loss of sensitive data [Storage.T31] |
|  |  |  |  |  |  |  |  |  | Exfiltrate data using blob inventory functionality [Storage.T24] |  |
|  |  |  |  |  |  |  |  |  | Unauthorized access to data using a rogue DFS endpoint [Storage.T30] |  |
|  |  |  |  |  |  |  |  |  | Unauthorized access to a sensitive message [Storage.T32] |  |

## 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 | class | Azure storage is Microsoft's cloud storage solution for modern data storage scenarios. Azure storage offers a massively scalable object store for data objects, a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store. |
| Key access feature | subclass of Storage account | When you create a storage account, Azure generates two 512-bit storage account access keys. These keys can be used to authorise access to data in your storage account via Shared Key authorization. Microsoft recommends that you use Azure Key Vault to manage your access keys, and that you regularly rotate and regenerate your keys. |
| File shares | subclass of Storage account | Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. |
| Monitoring | subclass of Storage account | Storage insights provides comprehensive monitoring of your Azure storage accounts by delivering a unified view of your Azure storage services performance, capacity, and availability. |
| Queues | subclass of Storage account | Azure queue storage is a service for storing large numbers of messages. Access messages via HTTP/S calls. |
| Replication | subclass of Storage account | Azure storage always stores multiple copies of data. It protects from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures. |
| Tables | subclass of Storage account | The most economic table style storage over the word to store petabytes of semi-structured data and keep costs down. |
| Blob storage, containers, data Lake storage Gen2 | subclass of Storage account | Data Lake storage Gen2 is the storage for big data analysis based on Azure blob storage. |
| Blob inventory | subclass of Blob storage, containers, data Lake storage Gen2 | 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 your total data size, age, encryption status, immutability policy, or legal hold. |
| Blob lifecycle | subclass of Blob storage, containers, data Lake storage Gen2 | Azure blob storage lifecycle management offers a rich, rule-based policy which you can use to transition your data to the best access tier and to expire data at the end of its lifecycle. |

| Storage account *(class, FC1)* *Azure storage is Microsoft's cloud storage solution for modern data storage scenarios. Azure storage offers a massively 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** | | --- | --- | | Creates a storage account with the specified parameters, updates the properties or tags, or adds a custom domain for the specified storage account. | Microsoft.Storage/storageAccounts/write | | Manage storage account migration to enable hierarchical namespace. | Microsoft.Storage/storageAccounts/accountMigration  s/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Man-in-the-middle attack via any storage account endpoint | [High (7.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) | | DDoS on endpoint | [Medium (5.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | | Use storage account name to steal data or distribute malicious data | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N) | | Exfiltrate data using different service | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) | | Unauthorized data exposed by breaking CORS settings | [Medium (4.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N) | | Unauthorised access to data by direct access to the physical disk | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Man-in-the-middle attack via any storage account endpoint

| | **Threat Id** | Storage.T11 | | --- | --- | | **Name** | Man-in-the-middle attack via any storage account endpoint | | **Description** | Storage account endpoints support HTTP/S. An attacker can intercept or modify the traffic via man-in-the-middle attack (e.g. with fake certificate to get and modify data in transit via endpoints). | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (7.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) | | **IAM Access** | {} | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce encryption-in-transit**    Maintain a list of authorized encryption in transit methods with desired assignment to storage accounts. Ideally minimum TLS 1.2.    Ensure authorized encryption in transit methods with desired assignment is set for authorized storage accounts.    Ensure storage accounts have authorized encryption in transit methods configured (e.g. using Azure Policy in deny mode).    Monitor the creation/update usage encryption in transit methods with desired assignment is set for authorized storage accounts (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly"). | Very High | 2 | 1 | 1 |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |

#### DDoS on endpoint

| | **Threat Id** | Storage.T29 | | --- | --- | | **Name** | DDoS on endpoint | | **Description** | An attacker can overload a public endpoint by a DDoS attack. If your application approaches or exceeds any of the scalability targets, it may encounter increased transaction latencies or throttling with 500 errors. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) | | **IAM Access** | {} | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)).    Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | High | 2 | 1 | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |

#### Use storage account name to steal data or distribute malicious data

| | **Threat Id** | Storage.T4 | | --- | --- | | **Name** | Use storage account name to steal data or distribute malicious data | | **Description** | Azure storage account names are globally unique. An attacker can take over an old account name, or delete an existing one, and entangle any third party to use their account to steal or distribute malicious data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N) | | **IAM Access** | {  "OPTIONAL": "Microsoft.Storage/storageAccounts/delete"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Very High | 1 | - | - |

#### Exfiltrate data using different service

| | **Threat Id** | Storage.T23 | | --- | --- | | **Name** | Exfiltrate data using different service | | **Description** | An attacker can exfiltrate data using different services (e.g. Azure data share, Logic App). Moreover these data can be stored in different subscriptions/tenants. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {  "AND": ["Microsoft.Storage/storageAccounts/write", "Microsoft.Authorization/role assignments/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Very High | 1 | - | - |

#### Unauthorized data exposed by breaking CORS settings

| | **Threat Id** | Storage.T26 | | --- | --- | | **Name** | Unauthorized data exposed by breaking 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 using the CORS misconfiguration can gain privileged access via origin reflection, enticing a user to access a page with a malicious script, returning sensitive data. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (4.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Govern Cross-Origin resource sharing**    Maintain a list of authorized CORS per endpoint trusted origins and corresponding settings.    Ensure only authorized storage accounts have CORS trusted origins and corresponding settings configured.    Prevent unauthorized storage accounts to use CORS trusted origins and corresponding settings (e.g. using Azure Policy in deny mode). | Very Low | 2 | 1 | - |

#### Unauthorised access to data by direct access to the physical disk

| | **Threat Id** | Storage.T14 | | --- | --- | | **Name** | Unauthorised access to data by direct access to the physical disk | | **Description** | Azure is operating the storage physical disks. An attacker (i.e. an Azure insider) can get access to data stored on the device. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {} | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce encryption-at-rest**    Maintain a list of authorized keys for Azure storage encryption with desired assignment and rotation policy.    Ensure authorized keys for Azure storage encryption with desired assignment and rotation policy is set for authorized storage accounts.    Ensure only authorized keys for Azure storage encryption with desired assignment and rotation policy are assigned (e.g. using Azure Policy in deny mode).    Monitor the creation/update and usage keys for Azure storage encryption with desired assignment and rotation policy assignment (e.g. using monitoring logs on authentication type in AccountKey). | High | 2 | 1 | 1 |
| **Apply cloud adoption, strategy, and governance**    Maintain a list of authorized Azure storage region options.    Ensure authorized Azure storage region is set for authorized storage accounts.    Ensure only authorized Azure storage region is set for authorized storage accounts (e.g. using Azure Policy in deny mode). | Low | 2 | 1 | - |
| **Protect primary data against loss**    Maintain a list of authorized Azure storage redundancy options.    Ensure authorized Azure storage redundancy is set for authorized storage accounts.    Ensure only authorized Azure storage redundancy is set for authorized storage accounts (e.g. using Azure Policy in deny mode). | Low | 2 | 1 | - |

| Key access feature *(subclass of Storage account, FC7)* *When you create a storage account, Azure generates two 512-bit storage account access keys. These keys can be used to authorise access to data in your storage account via Shared Key authorization. Microsoft recommends that you use Azure Key Vault to manage your access keys, and that you regularly rotate and regenerate your keys.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Returns the access keys for the specified storage account. | Microsoft.Storage/storageAccounts/listkeys/action | | Regenerates the access keys for the specified storage account. | Microsoft.Storage/storageAccounts/regeneratekey/ac  tion |  Threat List  | **Name** | **CVSS** | | --- | --- | | Exfiltrate data using account key access or SAS token | [High (8.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N) | | Privilege escalation accessing storage access key | [Medium (6.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) | | Block data access of a SAS token | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Exfiltrate data using account key access or SAS token

| | **Threat Id** | Storage.T3 | | --- | --- | | **Name** | Exfiltrate data using account key access or SAS token | | **Description** | Storage access keys have unrestricted access to the storage account they are coming from; SAS token can give access to a blob, directory, or file. An attacker can use a stolen storage account access key or SAS tokens to access confidential data, or modify data maliciously. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (8.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N) | | **IAM Access** | {} | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Managed Identity is the preferred method for accessing data Lake storage Gen2 from parent services.    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method.    Block the usage of storage account access key, whenever possible.    Maintain a revocation plan for any SAS or storage account access keys that you issue to clients based on requirements. If a SAS is compromised, you need to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas)).    Ensure the revocation plan is in place for any SAS or storage account access key. | Very High | 3 | 1 | - |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Maintain a list of authorized IPs to use SAS tokens, and their authorized time window.    Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS. | Medium | 2 | - | - |
| **Enable storage accounts monitoring & notifications**    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Low | 2 | 1 | - |
| **Enable soft-delete on containers, blobs, and file shares**    Ensure storage accounts have Azure Defender for Storage account enabled" with "Ensure storage accounts have Azure Defender for storage account enabled    Prevent the creation of storage accounts without Azure Defender for storage account option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode).    Ensure storage accounts have Azure Defender enabled    Prevent the creation of storage accounts without Azure Defender (e.g. by using an Azure Policy in deny mode). | Very Low | 2 | 2 | - |

#### Privilege escalation accessing storage access key

| | **Threat Id** | Storage.T1 | | --- | --- | | **Name** | Privilege escalation accessing storage access key | | **Description** | Storage accounts can have up to 2 access keys with unrestricted permissions on this storage account. An attacker can generate a new access key or use an existing key to gain unrestricted access. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (6.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/storageAccounts/rotateKey/action", "Microsoft.Storage/storageAccounts/revokeUserDelegationKeys/action", "Microsoft.Storage/storageAccounts/localusers/listKeys/action", "Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Ensure only authorized Groups are used in ACLs for data Lake storage Gen2.    Use name convention for Groups adding Suffix R/RW and Entity to be used.    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method.    Block the usage of storage account access key, whenever possible.    Maintain a revocation plan for any SAS or storage account access keys that you issue to clients based on requirements. If a SAS is compromised, you need to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas)).    Ensure the revocation plan is in place for any SAS or storage account access key. | Very High | 5 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS. | Medium | 1 | - | - |
| **Enable storage accounts monitoring & notifications**    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Low | 2 | 1 | - |

#### Block data access of a SAS token

| | **Threat Id** | Storage.T2 | | --- | --- | | **Name** | Block data access of a SAS token | | **Description** | SAS tokens are derived from an access key. Functionality is typically used by non-Azure applications to access data in a storage account. An attacker can rotate, or regenerate an access key to invalidate its SAS tokens to block data access to any applications using SAS tokens derived from this access key. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/storageAccounts/rotateKey/action", "Microsoft.Storage/storageAccounts/revokeUserDelegationKeys/action"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Ensure only authorized Groups are used in ACLs for data Lake storage Gen2.    Use name convention for Groups adding Suffix R/RW and Entity to be used.    Managed Identity is the preferred method for accessing data Lake storage Gen2 from parent services.    Block the usage of storage account access key, whenever possible.    Maintain a revocation plan for any SAS or storage account access keys that you issue to clients based on requirements. If a SAS is compromised, you need to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas)).    Ensure the revocation plan is in place for any SAS or storage account access key. | Very High | 6 | 1 | - |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)).    Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | High | 2 | 1 | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Enable soft-delete on containers, blobs, and file shares**    Ensure storage accounts have Azure Defender for Storage account enabled" with "Ensure storage accounts have Azure Defender for storage account enabled    Prevent the creation of storage accounts without Azure Defender for storage account option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode).    Ensure storage accounts have Azure Defender enabled    Prevent the creation of storage accounts without Azure Defender (e.g. by using an Azure Policy in deny mode). | Very Low | 2 | 2 | - |

| File shares *(subclass of Storage account, FC3)* *Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Create or update file share | Microsoft.Storage/storageAccounts/fileServices/sha  res/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Exfiltrate data using different access method | [High (7.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N) | | Usage outdated protocols to access file shares | [High (7.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) | | Privilege escalation by modifying file share ACL | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | Distribute malicious files via file share | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:L) | | Recursively delete directories and the content in the file share | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | Files encrypted by ransomware in file shares | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | Increase billing by file share overflow | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Exfiltrate data using different access method

| | **Threat Id** | Storage.T15 | | --- | --- | | **Name** | Exfiltrate data using different access method | | **Description** | Data stored on file share using SMB protocol can be accessible using HTTP/S protocol. An attacker can exfiltrate data using a different method of access (via blob access or static website endpoint) or an attacker can create an unauthorized DFS endpoint to gain access to the data in the blob. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (7.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/read", {  "AND": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/write"]  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)).    Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | High | 2 | 1 | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Define an ACL or IAM authentication for every data Lake storage Gen2. Ideally use Azure AD only, and multiple DLS if fine-grained access is required. | Medium | 1 | - | - |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2.    Ensure only authorized Groups are used in ACLs for data Lake storage Gen2.    Use name convention for Groups adding Suffix R/RW and Entity to be used.    Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method. | Low | 4 | - | - |
| **Ensure no storage account allow public access to blob**    Ensure no storage accounts have allowblobPublicAccess enabled, except if authorized.    Prevent the creation/update of storage accounts with allowblobPublicAccess enabled (e.g. using Azure Policy on deny mode - "[Preview]: storage account public access should be disallowed"). | Very Low | 1 | 1 | - |

#### Usage outdated protocols to access file shares

| | **Threat Id** | Storage.T21 | | --- | --- | | **Name** | Usage outdated protocols to access file shares | | **Description** | The primary reason to disable encryption in transit is to support a legacy application that must be run on an outdated operating system, such as Windows Server 2008 R2 or older Linux distribution. An attacker can hack old protocols and libraries to gain more permissions. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [High (7.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) | | **IAM Access** | {} | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce encryption-in-transit**    Maintain a list of authorized encryption in transit methods with desired assignment to storage accounts. Ideally minimum TLS 1.2.    Ensure authorized encryption in transit methods with desired assignment is set for authorized storage accounts.    Ensure storage accounts have authorized encryption in transit methods configured (e.g. using Azure Policy in deny mode).    Monitor the creation/update usage encryption in transit methods with desired assignment is set for authorized storage accounts (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly").    Maintain a list of authorized SMB 2.1 Azure Files.    Ensure only authorized Azure Files SMB 2.1 have encryption disabled.    Prevent unauthorized Azure Files SMB 2.1 to have encryption disabled (e.g. using Azure Policy in deny mode).    Monitor the creation/update of Azure Files SMB 2.1 and corresponding settings (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly"). | Very High | 4 | 2 | 2 |

#### Privilege escalation by modifying file share ACL

| | **Threat Id** | Storage.T17 | | --- | --- | | **Name** | Privilege escalation by modifying file share ACL | | **Description** | File share ACLs are used to limit access to entities via a file share endpoint. An attacker can modify those ACLs to escalate their own privileges. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write", "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/modifypermissions/action"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method.    Block the usage of storage account access key, whenever possible. | Low | - | 1 | - |
| **Protect primary data against loss**    Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs)) | Very Low | 1 | - | - |

#### Distribute malicious files via file share

| | **Threat Id** | Storage.T20 | | --- | --- | | **Name** | Distribute malicious files via file share | | **Description** | An attacker can distribute malicious and infected files via Windows shares. An attacker can infect underlying services (especially VMs) in that way. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0003](https://attack.mitre.org/tactics/TA0003) | | **CVSS** | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:L) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enable soft-delete on containers, blobs, and file shares**    For each file share, define the minimum retention of container and blob from the deletion (e.g. 7 days)    Ensure file shares have soft-delete enabled for at least the defined minimum retention    Prevent the creation of file shares without soft-delete (e.g. by using an Azure Policy in deny mode).    Ensure storage accounts have Azure Defender for Storage account enabled" with "Ensure storage accounts have Azure Defender for storage account enabled    Prevent the creation of storage accounts without Azure Defender for storage account option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode).    Ensure storage accounts have Azure Defender enabled    Prevent the creation of storage accounts without Azure Defender (e.g. by using an Azure Policy in deny mode). | Medium | 4 | 3 | - |
| **Protect primary data against loss**    Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs)) | Low | 1 | - | - |

#### Recursively delete directories and the content in the file share

| | **Threat Id** | Storage.T18 | | --- | --- | | **Name** | Recursively delete directories and the content in the file share | | **Description** | File share similar to the DFS has hierarchical architecture. An attacker can potentially delete multiple directories and files recursively. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/delete"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enable soft-delete on containers, blobs, and file shares**    For each file share, define the minimum retention of container and blob from the deletion (e.g. 7 days)    Ensure file shares have soft-delete enabled for at least the defined minimum retention    Prevent the creation of file shares without soft-delete (e.g. by using an Azure Policy in deny mode). | Medium | 2 | 1 | - |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method. | Low | - | - | - |
| **Protect primary data against loss**    Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs)) | Low | 1 | - | - |

#### Files encrypted by ransomware in file shares

| | **Threat Id** | Storage.T19 | | --- | --- | | **Name** | Files encrypted by ransomware in file shares | | **Description** | An attacker can encrypt files making them unusable in file share using an encryption key not controlled by the file owner, to request a ransom to access the decryption key. | | **Goal** | Direct Financial Gain | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "AND": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/read", "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write", "directory:W;file:W"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enable soft-delete on containers, blobs, and file shares**    For each file share, define the minimum retention of container and blob from the deletion (e.g. 7 days)    Ensure file shares have soft-delete enabled for at least the defined minimum retention    Prevent the creation of file shares without soft-delete (e.g. by using an Azure Policy in deny mode). | Medium | 2 | 1 | - |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method. | Low | - | - | - |
| **Protect primary data against loss**    Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs)) | Low | 1 | - | - |

#### Increase billing by file share overflow

| | **Threat Id** | Storage.T16 | | --- | --- | | **Name** | Increase billing by file share overflow | | **Description** | An attacker can upload terabytes to the file share and cause billing implication - especially with soft deleted option. | | **Goal** | Financial Drain | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N) | | **IAM Access** | {  "UNIQUE": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enable storage accounts monitoring & notifications**    Monitor file shares quotas and trends using Azure Monitor with alarm ([e.g. Azure file share size is 80% of capacity](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-monitoring?tabs=azure-portal#how-to-create-an-alert-if-the-azure-file-share-size-is-80-of-capacity)) | High | - | - | 1 |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method.    Block the usage of storage account access key, whenever possible.    Maintain a revocation plan for any SAS or storage account access keys that you issue to clients based on requirements. If a SAS is compromised, you need to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas)).    Ensure the revocation plan is in place for any SAS or storage account access key. | Very Low | 2 | 1 | - |

| Monitoring *(subclass of Storage account, FC8)* *Storage insights provides comprehensive monitoring of your Azure storage accounts by delivering a unified view of your Azure storage services performance, capacity, and availability.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates or updates the diagnostic setting for the resource. | Microsoft.Storage/storageAccounts/providers/Micros  oft.Insights/diagnosticsettings/write | | Creates or updates the diagnostic setting for the resource. | Microsoft.Storage/storageAccounts/blobServices/pro  viders/Microsoft.Insights/diagnosticsettings/write | | Creates or updates the diagnostic setting for the resource. | Microsoft.Storage/storageAccounts/tableServices/pr  oviders/Microsoft.Insights/diagnosticsettings/writ  e | | Creates or updates the diagnostic setting for the resource. | Microsoft.Storage/storageAccounts/fileServices/pro  viders/Microsoft.Insights/diagnosticsettings/write | | Creates or updates the diagnostic setting for the resource. | Microsoft.Storage/storageAccounts/queueServices/pr  oviders/Microsoft.Insights/diagnosticsettings/writ  e |  Threat List  | **Name** | **CVSS** | | --- | --- | | Exfiltrate data using diagnostic settings | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Exfiltrate data using diagnostic settings

| | **Threat Id** | Storage.T10 | | --- | --- | | **Name** | Exfiltrate data using diagnostic settings | | **Description** | Diagnostic settings can be set at storage account and/or blob level. An attacker can modify diagnostic settings, and send the storage accounts logs to another tenant/subscription to exfiltrate data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **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** |
| **Enable storage accounts monitoring & notifications**    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design.    Monitor the creation/update of storage accounts with diagnostic settings enabled (e.g. using activity logs on operation name - create or update resource diagnostic setting) | Very High | 2 | 1 | 1 |

| Queues *(subclass of Storage account, FC4)* *Azure queue storage is a service for storing large numbers of messages. Access messages via HTTP/S calls.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Create a queue | Microsoft.Storage/storageAccounts/queueServices/qu  eues/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Privilege escalation by modifying queue ACL | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | Unauthorized access to a sensitive message | [Medium (6.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) | | Impacting queues messages integrity or complete data loss of sensitive data | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Privilege escalation by modifying queue ACL

| | **Threat Id** | Storage.T27 | | --- | --- | | **Name** | Privilege escalation by modifying queue ACL | | **Description** | Queue ACLs are used to limit access to entities via the queue share endpoint. An attacker can modify those ACLs to escalate their own privileges. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/queueServices/write", "Microsoft.Storage/storageAccounts/queueServices/queues/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method.    Block the usage of storage account access key, whenever possible. | Low | - | 1 | - |

#### Unauthorized access to a sensitive message

| | **Threat Id** | Storage.T32 | | --- | --- | | **Name** | Unauthorized access to a sensitive message | | **Description** | An attacker can get access to the sensitive message or modify the message that will be consumed by other services and in that way access to other services. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (6.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/queueServices/write", "Microsoft.Storage/storageAccounts/queueServices/queues/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Very High | 1 | - | - |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)).    Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | High | 2 | 1 | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Maintain a list of authorized IPs to use SAS tokens, and their authorized time window.    Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS. | Medium | 2 | - | - |
| **Integrate ACLs in the IAM Operating Model to allow non-AD access files and directories**    Integrate the access to files and directories via ACL in the IAM Operating Model | Low | 1 | - | - |

#### Impacting queues messages integrity or complete data loss of sensitive data

| | **Threat Id** | Storage.T31 | | --- | --- | | **Name** | Impacting queues messages integrity or complete data loss of sensitive data | | **Description** | Messages in queues can be purged and deleted; queues can themselves be deleted with all the messages, and queues parameters changes can result in loss of all the messages. An attacker can delete or alter the messages and queues using any of those methods impacting downstream applications and processes and causing loss of integrity and DoS. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | | **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** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Very High | 1 | - | - |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)).    Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | High | 2 | 1 | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Maintain a list of authorized IPs to use SAS tokens, and their authorized time window.    Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS. | Medium | 2 | - | - |
| **Integrate ACLs in the IAM Operating Model to allow non-AD access files and directories**    Integrate the access to files and directories via ACL in the IAM Operating Model | Low | 1 | - | - |

| Replication *(subclass of Storage account, FC9)* *Azure storage always stores multiple copies of data. It protects from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Encryption | Microsoft.Storage/storageAccounts/encryptionScopes  /write | | Create or update object replication policy | Microsoft.Storage/storageAccounts/objectReplicatio  nPolicies/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Unauthorised access to data via storage account replication | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Unauthorised access to data via storage account replication

| | **Threat Id** | Storage.T13 | | --- | --- | | **Name** | Unauthorised access to data via storage account replication | | **Description** | Replication allows you to replicate objects and their metadata. At this moment it is not available for DFS, but in future will be, that can be additional attack vector. An attacker can configure replication on a storage account to replicate objects (or its metadata or tagging) to exfiltrate data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Protect primary data against loss**    Maintain a list of objects with cross-tenant replication enabled.    Ensure cross-tenant replication is allowed only for specific storage accounts. | Medium | 2 | - | - |
| **Enable storage accounts monitoring & notifications**    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Low | 2 | 1 | - |

| Tables *(subclass of Storage account, FC5)* *The most economic table style storage over the word to store petabytes of semi-structured data and keep costs down.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Create tables | Microsoft.Storage/storageAccounts/tableServices/ta  bles/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Privilege escalation by modifying table ACL | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Privilege escalation by modifying table ACL

| | **Threat Id** | Storage.T28 | | --- | --- | | **Name** | Privilege escalation by modifying table ACL | | **Description** | Table ACLs are used to limit access to entities via the table endpoint. An attacker can modify those ACLs to escalate their own privileges. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/tableServices/write", "Microsoft.Storage/storageAccounts/tableServices/tables/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method.    Block the usage of storage account access key, whenever possible. | Low | - | 1 | - |

| Blob storage, containers, data Lake storage Gen2 *(subclass of Storage account, FC2)* *Data Lake storage Gen2 is the storage for big data analysis based on Azure blob storage.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Create a filesystem rooted at the specified location. If the filesystem already exists, the operation fails. This operation does not support conditional HTTP requests. | Microsoft.Storage/storageAccounts/blobServices/con  tainers/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Unauthorized data made public | [High (8.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N) | | Unauthorized access to data using a rogue DFS endpoint | [High (7.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N) | | Distribute malicious infected files via a reputed web address | [High (7.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) | | Privilege escalation by modifying file system ACL | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | Files encrypted by ransomware in DFS/blob | [Medium (6.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H) | | Infect with malware downstream processes | [Medium (5.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:L/I:H/A:L) | | Unauthorised modification of data | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N) | | Recursively delete DFS directories and their content | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Unauthorized data made public

| | **Threat Id** | Storage.T5 | | --- | --- | | **Name** | Unauthorized data made public | | **Description** | An attacker (or someone by negligence) can create/modify a container to make it public and steal/exfiltrate/expose data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (8.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/blobServices/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Limit access to delete storage accounts, via Azure Policy and IAM. Do not ever delete a sensitive storage account (e.g. just delete all data) to make sure that storage account FQDN cannot be used as a source of attacks. | Very High | 1 | 1 | - |
| **Protect primary data against loss**    Maintain a list of objects with cross-tenant replication enabled.    Ensure cross-tenant replication is allowed only for specific storage accounts.    Maintain a list of authorized storage and corresponding accounts locks.    Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized storage accounts have lock disabled. | Very High | 4 | - | - |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    Maintain a list of authorized blob and containers with public access level set to anonymous, ideally none    Ensure anonymous access level is set only for authorized blobs / containers.    Ensure only authorized blob and containers are anonymously accessed (e.g. using Azure Policy in deny mode).    Monitor the creation/update of blob and containers that are anonymously accessed (e.g. using Azure Automations).    Ensure storage accounts have Azure Defender for Storage account enabled" with "Ensure storage accounts have Azure Defender for storage account enabled    Prevent the creation of storage accounts without Azure Defender for storage account option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode).    Ensure storage accounts have Azure Defender enabled    Prevent the creation of storage accounts without Azure Defender (e.g. by using an Azure Policy in deny mode). | High | 4 | 3 | 1 |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Define an ACL or IAM authentication for every data Lake storage Gen2. Ideally use Azure AD only, and multiple DLS if fine-grained access is required.    Use a data discovery tool to control that no sensitive data are stored in unauthorized storage account    Use a data discovery tool to ensure the storage account names, object names, and tags do not contain sensitive data | Medium | 1 | - | 2 |
| **Enable storage accounts monitoring & notifications**    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Low | 2 | 1 | - |
| **Ensure no storage account allow public access to blob**    Maintain a list of authorized storage accounts with allowblobPublicAccess enabled, ideally none    Ensure no storage accounts have allowblobPublicAccess enabled, except if authorized.    Prevent the creation/update of storage accounts with allowblobPublicAccess enabled (e.g. using Azure Policy on deny mode - "[Preview]: storage account public access should be disallowed"). | Low | 2 | 1 | - |

#### Unauthorized access to data using a rogue DFS endpoint

| | **Threat Id** | Storage.T30 | | --- | --- | | **Name** | Unauthorized access to data using a rogue DFS endpoint | | **Description** | An attacker can create an unauthorised DFS endpoint to gain access to the data in the blob. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (7.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N) | | **IAM Access** | {  "AND": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/write"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)).    Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | High | 2 | 1 | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Define an ACL or IAM authentication for every data Lake storage Gen2. Ideally use Azure AD only, and multiple DLS if fine-grained access is required. | Medium | 1 | - | - |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2.    Ensure only authorized Groups are used in ACLs for data Lake storage Gen2.    Use name convention for Groups adding Suffix R/RW and Entity to be used.    Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method. | Low | 4 | - | - |
| **Enable hierarchical namespace in storage account, only when required**    Maintain a list of authorized storage accounts with hierarchical namespace (DFS) option enabled.    Ensure only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured | Low | 2 | - | - |
| **Ensure no storage account allow public access to blob**    Ensure no storage accounts have allowblobPublicAccess enabled, except if authorized.    Prevent the creation/update of storage accounts with allowblobPublicAccess enabled (e.g. using Azure Policy on deny mode - "[Preview]: storage account public access should be disallowed"). | Very Low | 1 | 1 | - |

#### Distribute malicious infected files via a reputed web address

| | **Threat Id** | Storage.T22 | | --- | --- | | **Name** | Distribute malicious infected files via a reputed web address | | **Description** | Storage account can be configured as a static website server. An attacker can distribute malicious and infected files via a website hosted on a storage account. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0003](https://attack.mitre.org/tactics/TA0003) | | **CVSS** | [High (7.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Block access to the endpoints**    Maintain a list of authorized storage accounts has static website hosting option enabled, ideally none | High | 1 | - | - |
| **Ensure no storage account allow public access to blob**    Ensure only authorized storage accounts has the static website hosting option enabled.    Prevent unauthorized storage accounts to have the static website hosting option enabled (e.g. using Azure Policy on deny mode). | High | 1 | 1 | - |

#### Privilege escalation by modifying file system ACL

| | **Threat Id** | Storage.T6 | | --- | --- | | **Name** | Privilege escalation by modifying file system ACL | | **Description** | Filesystem ACLs are used to limit access to entities via the filesystem endpoint. An attacker can modify those ACLs to escalate their own privileges. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2.    Maintain an architecture of data Lake storage Gen2 ACL vs IAM based on requirements. Microsoft recommends using Azure Active Directory (Azure AD) to authorize requests against blob and queue data, if possible, instead of Shared Key. Azure AD provides superior security and ease of use over Shared Key.    Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method. | Very High | 4 | - | - |
| **Block access to the endpoints**    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 1 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    Ensure storage accounts have soft-delete for the blob enabled    Maintain a list of authorized blob and containers with public access level set to anonymous, ideally none    Ensure anonymous access level is set only for authorized blobs / containers.    Ensure only authorized blob and containers are anonymously accessed (e.g. using Azure Policy in deny mode).    Monitor the creation/update of blob and containers that are anonymously accessed (e.g. using Azure Automations). | High | 3 | 1 | 1 |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Protect primary data against loss**    Ensure cross-tenant replication is allowed only for specific storage accounts. | Medium | 1 | - | - |
| **Ensure no storage account allow public access to blob**    Prevent the creation/update of storage accounts with allowblobPublicAccess enabled (e.g. using Azure Policy on deny mode - "[Preview]: storage account public access should be disallowed"). | Low | - | 1 | - |
| **Enable hierarchical namespace in storage account, only when required**    Maintain a list of authorized storage accounts with hierarchical namespace (DFS) option enabled.    Ensure only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured | Low | 2 | - | - |

#### Files encrypted by ransomware in DFS/blob

| | **Threat Id** | Storage.T9 | | --- | --- | | **Name** | Files encrypted by ransomware in DFS/blob | | **Description** | An attacker can encrypt files/objects in DFS or blobs using an encryption key not controlled by the owner, to request a ransom to access the decryption key. | | **Goal** | Direct Financial Gain | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (6.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "directory:RWX;file:RWX"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Ensure only authorized Groups are used in ACLs for data Lake storage Gen2.    Use name convention for Groups adding Suffix R/RW and Entity to be used.    Maintain an architecture of data Lake storage Gen2 ACL vs IAM based on requirements. Microsoft recommends using Azure Active Directory (Azure AD) to authorize requests against blob and queue data, if possible, instead of Shared Key. Azure AD provides superior security and ease of use over Shared Key.    Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method.    Block the usage of storage account access key, whenever possible. | Very High | 5 | 1 | - |
| **Enable storage accounts monitoring & notifications**    Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob.    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Very High | 3 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS.    Use immutable blobs. | Very High | 2 | - | - |
| **Block access to the endpoints**    Maintain a list of IPs authorized to access each storage account.    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Protect primary data against loss**    Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, DFS, including regular testing. | Medium | 1 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    For each storage account (or type of data), define the minimum retention of container and blob from the deletion (e.g. 7 days)    Ensure storage accounts have soft-delete for the blob enabled for at least the defined minimum retention    Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy in deny mode).    Ensure storage accounts have soft-delete for the container enabled    Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode).    Ensure storage accounts have soft-delete for the blob enabled    Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode).    Ensure storage accounts have soft-delete for the container enabled    Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode). | Medium | 5 | 4 | - |
| **Integrate ACLs in the IAM Operating Model to allow non-AD access files and directories**    Integrate the access to files and directories via ACL in the IAM Operating Model | Very Low | 1 | - | - |

#### Infect with malware downstream processes

| | **Threat Id** | Storage.T12 | | --- | --- | | **Name** | Infect with malware downstream processes | | **Description** | An attacker can distribute malicious and infected files via an object used by downstream services or a reputed company URL. An attacker can upload a malware instead of a valid file, and infect internal services or external users. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0003](https://attack.mitre.org/tactics/TA0003) | | **CVSS** | [Medium (5.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:L/I:H/A:L) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Managed Identity is the preferred method for accessing data Lake storage Gen2 from parent services.    Block the usage of storage account access key, whenever possible. | Very High | 2 | 1 | - |
| **Enable storage accounts monitoring & notifications**    Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob. | Very High | 1 | - | - |
| **Scan input/output objects for malware**    If the storage account is used as an input or the output of a process, scan the objects for malware (e.g. using VirusScan) | High | - | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS.    Use immutable blobs. | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint.    Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS.    Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | High | 2 | 1 | - |
| **Block access to the endpoints**    Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | Medium | 1 | - | - |
| **Protect primary data against loss**    Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, DFS, including regular testing. | Medium | 1 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    For each storage account (or type of data), define the minimum retention of container and blob from the deletion (e.g. 7 days)    Ensure storage accounts have soft-delete for the blob enabled for at least the defined minimum retention    Ensure storage accounts have soft-delete for the container enabled    Ensure storage accounts have soft-delete for the blob enabled    Ensure storage accounts have soft-delete for the container enabled | Medium | 5 | - | - |

#### Unauthorised modification of data

| | **Threat Id** | Storage.T8 | | --- | --- | | **Name** | Unauthorised modification of data | | **Description** | Common scenario for data Lake storage Gen2 is that incoming data after uploading to blob storage should not be modified. An attacker can modify data that can cause inconsistency in dependent subsystems. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2. | Very High | 2 | - | - |
| **Enable storage accounts monitoring & notifications**    Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob.    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Very High | 3 | 1 | - |
| **Identify and ensure the protection all storage accounts hosting your objects**    Use immutable blobs. | Very High | 1 | - | - |

#### Recursively delete DFS directories and their content

| | **Threat Id** | Storage.T7 | | --- | --- | | **Name** | Recursively delete DFS directories and their content | | **Description** | DFS has a hierarchical architecture. An attacker can potentially delete multiple directories and files recursively to make them unavailable. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "UNIQUE": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel.    Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2.    Ensure only authorized Groups are used in ACLs for data Lake storage Gen2.    Use name convention for Groups adding Suffix R/RW and Entity to be used.    Maintain an architecture of data Lake storage Gen2 ACL vs IAM based on requirements. Microsoft recommends using Azure Active Directory (Azure AD) to authorize requests against blob and queue data, if possible, instead of Shared Key. Azure AD provides superior security and ease of use over Shared Key.    Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method. | Very High | 6 | - | - |
| **Enable storage accounts monitoring & notifications**    Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob.    Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving.    Ensure diagnostic settings are configured properly to the architecture design.    Ensure storage accounts have diagnostic settings configured according to the design. | Very High | 3 | 1 | - |
| **Integrate ACLs in the IAM Operating Model to allow non-AD access files and directories**    Integrate the access to files and directories via ACL in the IAM Operating Model | Very High | 1 | - | - |
| **Protect primary data against loss**    Enable versioning on blobs holding primary data    Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs))    Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, DFS, including regular testing. | Medium | 3 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    For each storage account (or type of data), define the minimum retention of container and blob from the deletion (e.g. 7 days)    Ensure storage accounts have soft-delete for the blob enabled for at least the defined minimum retention    Ensure storage accounts have soft-delete for the container enabled    Ensure storage accounts have soft-delete for the blob enabled    Ensure storage accounts have soft-delete for the container enabled | Medium | 5 | - | - |
| **Enable hierarchical namespace in storage account, only when required**    Maintain a list of authorized storage accounts with hierarchical namespace (DFS) option enabled.    Ensure only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured | Low | 2 | - | - |

| Blob inventory *(subclass of Blob storage, containers, data Lake storage Gen2, 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 your total data size, age, encryption status, immutability policy, or legal hold.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Policies write | Microsoft.Storage/storageAccounts/inventoryPolicie  s/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Exfiltrate data using blob inventory functionality | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Exfiltrate data using blob inventory functionality

| | **Threat Id** | Storage.T24 | | --- | --- | | **Name** | Exfiltrate data using blob inventory functionality | | **Description** | An attacker can setup/modify and get access to blob inventory and in that way get knowledge about running services and exfiltrate data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/inventoryPolicies/read", "Microsoft.Storage/storageAccounts/inventoryPolicies/write", "Microsoft.Storage/storageAccounts/inventoryPolicies/delete"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Very High | 1 | - | - |

| Blob lifecycle *(subclass of Blob storage, containers, data Lake storage Gen2, FC6)* *Azure blob storage lifecycle management offers a rich, rule-based policy which you can use to transition your data to the best access tier and to expire data at the end of its lifecycle.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Set blob container legal hold | Microsoft.Storage/storageAccounts/blobServices/con  tainers/setLegalHold/action | | Put blob container immutability policy | Microsoft.Storage/storageAccounts/blobServices/con  tainers/immutabilityPolicies/write |  Threat List  | **Name** | **CVSS** | | --- | --- | | Recursively delete data using blob storage lifecycle management | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Recursively delete data using blob storage lifecycle management

| | **Threat Id** | Storage.T25 | | --- | --- | | **Name** | Recursively delete data using blob storage lifecycle management | | **Description** | An attacker can setup/modify blob storage lifecycle management and in that way delete data, even after a time. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/clearLegalHold/action", "Microsoft.Storage/storageAccounts/blobServices/containers/setLegalHold/action", "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/extend/action", "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/delete", "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/write", "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/lock/action", "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/read"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Limit the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Very High | 1 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    Ensure storage accounts have soft-delete for the blob enabled    Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode).    Ensure storage accounts have soft-delete for the container enabled    Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode). | Medium | 2 | 2 | - |

# Control Implementation

## Limit the IAM entities allowed to execute the IAM actions required to perform 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 the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Request the list of authorized IAM principals that have the permissions required to launch attacks, its review process, and its review records. | Medium | Storage.FC1  Storage.FC10  Storage.FC2  Storage.FC4  Storage.FC6  Storage.FC7 | Storage.T1 (Medium)  Storage.T2 (Medium)  Storage.T4 (Medium)  Storage.T5 (Medium)  Storage.T6 (Medium)  Storage.T7 (Medium)  Storage.T8 (Medium)  Storage.T9 (Medium)  Storage.T12 (Medium)  Storage.T23 (High)  Storage.T24 (Medium)  Storage.T25 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C23]  Limit access to delete storage accounts, via Azure Policy and IAM. Do not ever delete a sensitive storage account (e.g. just delete all data) to make sure that storage account FQDN cannot be used as a source of attacks. | Try to delete storage account, it should be denied | Medium | Storage.FC2 | Storage.T5 (Very High) | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C27]  Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2. | Request the list of authorized Groups, its review process, and its review records. | Very Low | Storage.FC2  Storage.FC3 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C28, depends on Storage.C27]  Ensure only authorized Groups are used in ACLs for data Lake storage Gen2. | Review ACLs against usage of individual users' service principal. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T30 (Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C29, depends on Storage.C27]  Use name convention for Groups adding Suffix R/RW and Entity to be used. | Review Group-Name convention. | Medium | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T30 (Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C32]  Maintain an architecture of data Lake storage Gen2 ACL vs IAM based on requirements. Microsoft recommends using Azure Active Directory (Azure AD) to authorize requests against blob and queue data, if possible, instead of Shared Key. Azure AD provides superior security and ease of use over Shared Key. | Check documentation. | Medium | Storage.FC2 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T9 (Very Low) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C33, depends on Storage.C32]  Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method. | Request the IAM operating model for the directories and objects. | Low | Storage.FC2  Storage.FC3 | Storage.T6 (Very Low)  Storage.T7 (High)  Storage.T9 (High)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C44]  Managed Identity is the preferred method for accessing data Lake storage Gen2 from parent services. | Check if underlying services are not using SAS, or other password methods to authenticate. | Medium | Storage.FC2  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T12 (High) | Medium |
| Corrective (COSO)  Protect (NIST CSF) | [Storage.C81]  Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method. | Check if (Azure) Active Directory is used for assigning permissions. | Medium | Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | Storage.T1 (Low)  Storage.T3 (Low)  Storage.T16 (Very Low)  Storage.T17 (Low)  Storage.T18 (Low)  Storage.T19 (Low)  Storage.T27 (Low)  Storage.T28 (Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C82, assured by Storage.C83]  Block the usage of storage account access key, whenever possible. | Try to connect using storage account access keys - Expected error "key based authentication is not permitted on this storage account", it should be denied. | Medium | Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | Storage.T1 (Very High)  Storage.T2 (Very High)  Storage.T3 (Very High)  Storage.T9 (Very Low)  Storage.T12 (Very High)  Storage.T16 (Very Low)  Storage.T17 (Low)  Storage.T27 (Low)  Storage.T28 (Low) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C83]  Verify only authorized authorization method set for authorized blob, file shares, queues, tables, DFS (e.g. using Azure Policy on audit mode). | Configure a blob, file share, queue, table, or DFS with an unauthorized authorization method, it should be detected. | High | Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C89]  Maintain a revocation plan for any SAS or storage account access keys that you issue to clients based on requirements. If a SAS is compromised, you need to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas)). | Request the of authorized revocation plan for any SAS or storage account access keys, its review process, and its review records. | Low | Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C90, depends on Storage.C89, assured by Storage.C91]  Ensure the revocation plan is in place for any SAS or storage account access key. | Request 1) the mechanism ensuring revocation plan in place for any SAS or storage account access keys is in use, 2) its records of testing for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C91]  Verify the revocation plan is in place for any SAS or storage account access key. | Check test executions. Any unsuccessful attempts, it should be detected | High | Storage.FC3  Storage.FC7 | - | Low |

## Identify and ensure the protection all storage accounts hosting your objects [Storage.CO2]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C2]  Define an ACL or IAM authentication for every data Lake storage Gen2. Ideally use Azure AD only, and multiple DLS if fine-grained access is required. | Request the list of all storage accounts you control, define their authorized data classification, identify whether the data is primary and the mechanism and records to ensure the accuracy of those metadata | High | Storage.FC2  Storage.FC3 | Storage.T5 (Very Low)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C3, depends on Storage.C2]  Use a data discovery tool to control that no sensitive data are stored in unauthorized storage account | Upload a higher classification data in a storage account, it should be detected. | Medium | Storage.FC2 | Storage.T5 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C4]  Use a data discovery tool to ensure the storage account names, object names, and tags do not contain sensitive data | Create 1) a storage account name, 2) object names, or 3) tags with sensitive data, it should be detected. | Very High | Storage.FC2 | Storage.T5 (Medium) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C24]  Maintain a list of authorized IPs to use SAS tokens, and their authorized time window. | Request the list of authorized IPs to use SAS tokens, its review process, and its review records. | Very Low | Storage.FC4  Storage.FC7 | Storage.T3 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C25, depends on Storage.C24, assured by Storage.C26]  Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS. | Request 1) the mechanism ensuring SAS tokens allow only authorized IPs, 2) its records of execution for all new SAS tokens, and 3) plan to move any older SAS tokens. | Very Low | Storage.FC2  Storage.FC4  Storage.FC7 | Storage.T1 (Low)  Storage.T3 (Low)  Storage.T9 (Very Low)  Storage.T12 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C26]  Verify SAS tokens only allow authorized IPs. | Deploy a SAS token with an unauthorized IP, it should be detected | Medium | Storage.FC2  Storage.FC4  Storage.FC7 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C31, depends on Storage.C30]  Use immutable blobs. | Check the usage of immutable blobs. | Medium | Storage.FC2 | Storage.T8 (Very High)  Storage.T9 (Very High)  Storage.T12 (Medium) | High |

## Integrate ACLs in the IAM Operating Model to allow non-AD access files and directories [Storage.CO3]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C5, depends on Storage.C1]  Integrate the access to files and directories via ACL in the IAM Operating Model | Request the IAM operating model for the access to files and directories via ACL | Low | Storage.FC2  Storage.FC4 | Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T31 (Low)  Storage.T32 (Low) | High |

## Ensure no storage account allow public access to blob [Storage.CO4]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C6]  Maintain a list of authorized storage accounts with allowblobPublicAccess enabled, ideally none | Request the list of authorized storage accounts with allowblobPublicAccess enabled, its review process, and its review records. | Low | Storage.FC2 | Storage.T5 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C7, depends on Storage.C6, assured by Storage.C9]  Ensure no storage accounts have allowblobPublicAccess enabled, except if authorized. | Request 1) the mechanism ensuring only authorized storage accounts have allowblobPublicAccess enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2  Storage.FC3 | Storage.T5 (Medium)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C8, depends on Storage.C6]  Prevent the creation/update of storage accounts with allowblobPublicAccess enabled (e.g. using Azure Policy on deny mode - "[Preview]: storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be denied. | High | Storage.FC2  Storage.FC3 | Storage.T5 (Medium)  Storage.T6 (Medium)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C9]  Verify no storage accounts have allowblobPublicAccess enabled (e.g. using Azure Policy on audit mode - "[Preview]: storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be detected. | High | Storage.FC2  Storage.FC3 | - | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C52]  Verify storage accounts with cross-tenant replication enabled (e.g. using Azure Policy "storage accounts should prevent cross tenant object replication" in audit mode.). | Creation of storage account with cross-tenant option enabled, it should be detected. | Low | Storage.FC2  Storage.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C93, depends on Storage.C92, assured by Storage.C95]  Ensure only authorized storage accounts has the static website hosting option enabled. | Request 1) the mechanism ensuring only authorized storage accounts has static website hosting option enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2 | Storage.T22 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C94, depends on Storage.C92]  Prevent unauthorized storage accounts to have the static website hosting option enabled (e.g. using Azure Policy on deny mode). | Create a storage account with a static website hosting option enabled, it should be denied. | Very Low | Storage.FC2 | Storage.T22 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C95]  Verify only authorized storage accounts has the static website hosting option enabled (e.g. using Azure Policy on audit mode). | Create a storage account with a static website hosting option enabled, it should be detected. | High | Storage.FC2 | - | Medium |

## Protect primary data against loss [Storage.CO5]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C10, assured by Storage.C11]  Enable versioning on blobs holding primary data | Request the mechanism used to ensure versioning on blobs holding primary data, and its records | Medium | Storage.FC2 | Storage.T7 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C11]  Verify blobs holding primary data are versioned | Remove versioning from a blob holding primary data, it should be detected | High | Storage.FC2 | - | Low |
| Directive (COSO)  Recover (NIST CSF) | [Storage.C12]  Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs)) | Request the mechanism used to backup primary data in a location which have different security authority, its records of execution, and records of restoration testing | High | Storage.FC2  Storage.FC3 | Storage.T7 (High)  Storage.T17 (Low)  Storage.T18 (Medium)  Storage.T19 (Medium)  Storage.T20 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C49]  Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, DFS, including regular testing. | Request the backup policies for DFS, its review process, and its review records. | Low | Storage.FC2 | Storage.T7 (Medium)  Storage.T9 (Medium)  Storage.T12 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C50]  Maintain a list of objects with cross-tenant replication enabled. | Request the list of authorized objects use allow cross-tenant replication, its review process, and its review records. | Low | Storage.FC2  Storage.FC9 | Storage.T5 (Very Low)  Storage.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C51, depends on Storage.C50, assured by Storage.C52]  Ensure cross-tenant replication is allowed only for specific storage accounts. | Request 1) the mechanism ensuring allowblobPublicAccess allow only authorized blobs, 2) its records of execution for all new blobs. | High | Storage.FC2  Storage.FC9 | Storage.T5 (High)  Storage.T6 (High)  Storage.T13 (High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C73]  Maintain a list of authorized Azure storage redundancy options. | Request the list of authorized Azure storage redundancy, its review process, and its review records. | Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C74, depends on Storage.C73, assured by Storage.C76]  Ensure authorized Azure storage redundancy is set for authorized storage accounts. | Request 1) the mechanism ensuring only Azure storage redundancy for storage accounts are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC1 | Storage.T14 (Very Low) | Very Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C75, depends on Storage.C73]  Ensure only authorized Azure storage redundancy is set for authorized storage accounts (e.g. using Azure Policy in deny mode). | Create a blob with unauthorized Azure storage redundancy for Azure storage, it should be denied. | Very Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C76]  Verify only authorized Azure storage redundancy is set for authorized storage accounts (e.g. using Azure Policy on audit mode). | Configure a storage account with an unauthorized redundancy settings, it should be detected. | High | Storage.FC1 | - | Very Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C111]  Maintain a list of authorized storage and corresponding accounts locks. | Request the list of authorized storage accounts locks settings, its review process, and its review records. | Very Low | Storage.FC2 | Storage.T5 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C112, depends on Storage.C111, assured by Storage.C113]  Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized storage accounts have lock disabled. | Request 1) the mechanism ensuring only authorized storage accounts have locks disabled, 2) its records of execution for all new storage accounts locks, and 3) plan to move any older storage accounts | Very Low | Storage.FC2 | Storage.T5 (High) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C113]  Verify the creation/update of storage accounts lock and corresponding settings (e.g. using activity logs "localized Value": "Delete management locks"). | Delete a storage account lock, it should be detected. | Very Low | Storage.FC2 | - | Very High |

## Enable soft-delete on containers, blobs, and file shares [Storage.CO6]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C13]  For each storage account (or type of data), define the minimum retention of container and blob from the deletion (e.g. 7 days) | For each storage account, request the minimum retention of container and blob from the deletion, its review process, and its review records | Low | Storage.FC2 | Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C14, depends on Storage.C13, assured by Storage.C16]  Ensure storage accounts have soft-delete for the blob enabled for at least the defined minimum retention | Request 1) the mechanism ensuring storage accounts have soft-delete for the blob enabled for at least the defined minimum retention, 2) its records of execution for all new storage accounts, and 3) 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.C15, depends on Storage.C13]  Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy in deny mode). | Create a storage account without soft-delete for the blob, it should be denied | High | Storage.FC2 | Storage.T9 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C16]  Verify all storage accounts have soft-delete for the blob enabled (e.g. by using an Azure Policy in audit mode). | Create a storage account without soft-delete for the blob option, it should be detected. | Low | Storage.FC2 | - | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C17, depends on Storage.C13, assured by Storage.C19]  Ensure storage accounts have soft-delete for the container enabled | Request 1) the mechanism ensuring storage accounts have soft-delete for the container enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC2 | Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low) | Very Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C18, depends on Storage.C13]  Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode). | Create a storage account without soft-delete for the container, it should be denied. | High | Storage.FC2 | Storage.T9 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C19]  Verify storage accounts without soft-delete for the container are not configured. | Create a storage account without soft-delete for the container option, it should be detected. | Low | Storage.FC2 | - | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C34, assured by Storage.C36]  Ensure storage accounts have soft-delete for the blob enabled | Request 1) the mechanism ensuring storage accounts have soft-delete for the blob enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2  Storage.FC6 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T25 (Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C35]  Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode). | Create a storage account without soft-delete for the blob, it should be denied | High | Storage.FC2  Storage.FC6 | Storage.T9 (High)  Storage.T25 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C36]  Verify all storage accounts have soft-delete for the blob enabled | Create a storage account without soft-delete for the blob option, it should be detected. | Low | Storage.FC2  Storage.FC6 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C37, assured by Storage.C39]  Ensure storage accounts have soft-delete for the container enabled | Request 1) the mechanism ensuring storage accounts have soft-delete for the container enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC2  Storage.FC6 | Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T25 (Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C38, depends on Storage.C34]  Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode). | Create a storage account without soft-delete for the container, it should be denied. | High | Storage.FC2  Storage.FC6 | Storage.T9 (High)  Storage.T25 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C39]  Verify storage accounts without soft-delete for the container are not configured. | Create a storage account without soft-delete for the container option, it should be detected. | Low | Storage.FC2  Storage.FC6 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C58]  Maintain a list of authorized blob and containers with public access level set to anonymous, ideally none | Request the list of authorized blob and containers with public access level set to anonymous, its review process, and its review records. | Low | Storage.FC2 | Storage.T5 (Very Low)  Storage.T6 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C59, depends on Storage.C58, assured by Storage.C62]  Ensure anonymous access level is set only for authorized blobs / containers. | Request 1) the mechanism ensuring only authorized blob / container are anonymously accessed, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2 | Storage.T5 (Medium)  Storage.T6 (Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C60, depends on Storage.C58]  Ensure only authorized blob and containers are anonymously accessed (e.g. using Azure Policy in deny mode). | Create a blob, or a container anonymously accessible, it should be denied. | Very Low | Storage.FC2 | Storage.T5 (Medium)  Storage.T6 (Low) | High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C61]  Monitor the creation/update of blob and containers that are anonymously accessed (e.g. using Azure Automations). | Create a blob, or a container anonymously accessible, it should be detected. | Low | Storage.FC2 | Storage.T5 (Medium)  Storage.T6 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C62]  Verify only authorized blob or containers are anonymously accessible (e.g. using Azure Policy on audit mode). | Create 1) a blob, or 2) a container anonymously accessible, it should be detected. | High | Storage.FC2 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C85]  For each file share, define the minimum retention of container and blob from the deletion (e.g. 7 days) | For each file share, request the minimum retention from the deletion, its review process, and its review records | High | Storage.FC3 | Storage.T18 (Very Low)  Storage.T19 (Very Low)  Storage.T20 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C86, depends on Storage.C85, assured by Storage.C88]  Ensure file shares have soft-delete enabled for at least the defined minimum retention | Request 1) the mechanism ensuring file shares have soft-delete enabled for at least the defined minimum retention, 2) it's records of execution for all new file shares, and 3) plan to move any older file shares | Low | Storage.FC3 | Storage.T18 (Medium)  Storage.T19 (Very Low)  Storage.T20 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C87, depends on Storage.C85]  Prevent the creation of file shares without soft-delete (e.g. by using an Azure Policy in deny mode). | Create a file share without soft-delete, it should be denied | High | Storage.FC3 | Storage.T18 (Medium)  Storage.T19 (Very Low)  Storage.T20 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C88]  Verify all file shares have soft-delete (e.g. by using an Azure Policy in audit mode). | Create a file share without soft-delete , it should be detected. | Low | Storage.FC3 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C105, assured by Storage.C107]  Ensure storage accounts have Azure Defender for Storage account enabled" with "Ensure storage accounts have Azure Defender for storage account enabled | Request 1) the mechanism ensuring storage accounts have Azure Defender for storage account enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C106]  Prevent the creation of storage accounts without Azure Defender for storage account option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode). | Create a storage account without Azure Defender for storage account, it should be denied | High | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C107]  Verify all storage accounts have Azure Defender for storage account enabled | Create a storage account without Azure Defender for storage account option, it should be detected. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C108, assured by Storage.C110]  Ensure storage accounts have Azure Defender enabled | Request 1) the mechanism ensuring storage accounts have Azure Defender for storage account enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C109, depends on Storage.C105]  Prevent the creation of storage accounts without Azure Defender (e.g. by using an Azure Policy in deny mode). | Create a storage account without Azure Defender for storage account, it should be denied. | High | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C110]  Verify storage accounts without Azure Defender for storage account enabled. | Create a storage account without Azure Defender for storage account, it should be detected. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | - | Medium |

## Enable hierarchical namespace in storage account, only when required [Storage.CO7]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C20]  Maintain a list of authorized storage accounts with hierarchical namespace (DFS) option enabled. | Request the list of authorized {resources}, its review process, and its review records | Medium | Storage.FC2 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C21, depends on Storage.C20, assured by Storage.C22]  Ensure only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured | Request 1) the mechanism ensuring only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured, 2) its records of execution for all new storage accounts with hierarchical namespace (DFS) option enabled and 3) plan to move any older storage accounts with hierarchical namespace (DFS) option enabled. | Medium | Storage.FC2 | Storage.T6 (Low)  Storage.T7 (Low)  Storage.T30 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C22]  Verify storage accounts with hierarchical namespace (DFS) option enabled are not configured (e.g. by using an Azure Policy {"isHnsEnabled": "true"} in audit mode) | Create a storage account with hierarchical namespace (DFS) option enabled, 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** |
| --- | --- | --- | --- | --- | --- | --- |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C67]  Verify only authorized keys for Azure storage encryption with desired assignment and rotation policy are in use (e.g. using Azure Policy on audit mode). | Configure a storage account with an unauthorized encryption settings, it should be detected. | High | Storage.FC1 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C68]  Maintain a list of authorized encryption in transit methods with desired assignment to storage accounts. Ideally minimum TLS 1.2. | Request the list of authorized encryption in transit methods, its review process, and its review records. | Very Low | Storage.FC1  Storage.FC3 | Storage.T11 (Very Low)  Storage.T21 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C69, depends on Storage.C68, assured by Storage.C72]  Ensure authorized encryption in transit methods with desired assignment is set for authorized storage accounts. | Request 1) the mechanism ensuring only encryption in transit methods with desired assignment are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Low | Storage.FC1  Storage.FC3 | Storage.T11 (High)  Storage.T21 (Medium) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C70, depends on Storage.C68]  Ensure storage accounts have authorized encryption in transit methods configured (e.g. using Azure Policy in deny mode). | Create a blob with unauthorized encryption in transit methods for Azure storage, it should be denied. | Medium | Storage.FC1  Storage.FC3 | Storage.T11 (Very High)  Storage.T21 (Medium) | Very High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C71]  Monitor the creation/update usage encryption in transit methods with desired assignment is set for authorized storage accounts (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly"). | Configure a storage account with an unauthorized encryption in transit settings, it should be detected. | Low | Storage.FC1  Storage.FC3 | Storage.T11 (Medium)  Storage.T21 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C72]  Verify only authorized encryption in transit methods with desired assignment is set for authorized storage accounts (e.g. using Azure Policy on audit mode). | Configure a storage account with an unauthorized encryption in transit settings, it should be detected. | Low | Storage.FC1  Storage.FC3 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C100]  Maintain a list of authorized SMB 2.1 Azure Files. | Request the list of authorized SMB 2.1 Azure Files with SMB 2.1 settings, its review process, and its review records. | Low | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C101, depends on Storage.C100, assured by Storage.C104]  Ensure only authorized Azure Files SMB 2.1 have encryption disabled. | Request 1) the mechanism ensuring only authorized SMB 2.1 Azure Files have encryption disabled, 2) its records of execution for all new SMB 2.1 Azure Files, and 3) plan to move any older storage accounts | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C102, depends on Storage.C100]  Prevent unauthorized Azure Files SMB 2.1 to have encryption disabled (e.g. using Azure Policy in deny mode). | Create a storage account with encryption disabled, it should be denied. | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C103]  Monitor the creation/update of Azure Files SMB 2.1 and corresponding settings (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly"). | Create a storage account with encryption disabled, it should be detected. | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C104]  Verify only authorized Azure Files SMB 2.1 and corresponding settings are configured (e.g. using Azure Policy on audit mode). | Create a storage account with encryption disabled, it should be detected. | High | Storage.FC3 | - | Low |

## Connect via private endpoint [Storage.CO9]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C40]  Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint. | Request the list of authorized IPs, its review process, and its review records. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T6 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T12 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T30 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C41, depends on Storage.C40, assured by Storage.C43]  Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS. | Request 1) the mechanism ensuring PE are in place 2) its records of execution for all new DFS. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T6 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Low)  Storage.T29 (Low)  Storage.T30 (Low)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C42, depends on Storage.C40]  Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | Configure an unauthorized VNETs on a storage account, it should be denied. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T6 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T30 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C43]  Verify the unauthorized VNETs cannot access to the storage account. | Configure an unauthorized VNETs on a storage account, it should be detected. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | - | High |

## Block access to the endpoints [Storage.CO10]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C45]  Maintain a list of IPs authorized to access each storage account. | Request the list of authorized blobs to use allowblobPublicAccess enabled, its review process, and its review records. | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T30 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C46, depends on Storage.C45, assured by Storage.C48]  Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | Request 1) the mechanism ensuring firewall rules are in place 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (High)  Storage.T3 (High)  Storage.T5 (High)  Storage.T6 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T30 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C47, depends on Storage.C45]  Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | Access from unauthorized IPs, it should be denied. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very Low)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T30 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C48]  Verify access is possible only from allowed list (e.g. by using Azure Policy) | Connect to storage from not allowed IP, it should be detected. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | - | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C92]  Maintain a list of authorized storage accounts has static website hosting option enabled, ideally none | Request the list of authorized storage accounts with static website hosting option enabled, its review process, and its review records. | Low | Storage.FC2 | Storage.T22 (Very Low) | High |

## Enable storage accounts monitoring & notifications [Storage.CO11]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C30]  Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob. | Request the list of directories and blobs for immutable blobs functionality. | Medium | Storage.FC2 | Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C53]  Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving. | Request the design of diagnostic settings for storage accounts, its review process, and its review records. | Low | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T10 (Very Low)  Storage.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C54, depends on Storage.C53, assured by Storage.C57]  Ensure diagnostic settings are configured properly to the architecture design. | Request 1) the mechanism ensuring only authorized diagnostic settings destinations are enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Low | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T10 (Medium)  Storage.T13 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C55, depends on Storage.C53]  Ensure storage accounts have diagnostic settings configured according to the design. | Create a storage account with on approved diagnostic settings options, it should be denied. | Very Low | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T10 (High)  Storage.T13 (Very Low) | High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C56]  Monitor the creation/update of storage accounts with diagnostic settings enabled (e.g. using activity logs on operation name - create or update resource diagnostic setting) | Configure a storage account with an unauthorized diagnostic settings options, it should be detected. | Low | Storage.FC8 | Storage.T10 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C57]  Verify storage accounts have diagnostic settings configured according to the design (e.g. using 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. | High | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | - | Medium |
| Detective (COSO)  Protect (NIST CSF) | [Storage.C84]  Monitor file shares quotas and trends using Azure Monitor with alarm ([e.g. Azure file share size is 80% of capacity](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-monitoring?tabs=azure-portal#how-to-create-an-alert-if-the-azure-file-share-size-is-80-of-capacity)) | Create a file with unauthorized or default quota, it should be detected. | Very Low | Storage.FC3 | Storage.T16 (Medium) | Low |

## Enforce encryption-at-rest [Storage.CO12]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C63]  Maintain a list of authorized keys for Azure storage encryption with desired assignment and rotation policy. | Request the list of authorized keys for Azure storage encryption with desired assignment and rotation policy, its review process, and its review records. | Low | Storage.FC1 | Storage.T14 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C64, depends on Storage.C63, assured by Storage.C67]  Ensure authorized keys for Azure storage encryption with desired assignment and rotation policy is set for authorized storage accounts. | Request 1) the mechanism ensuring only authorized keys for Azure storage encryption with desired assignment and rotation policy are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC1 | Storage.T14 (Medium) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C65, depends on Storage.C63]  Ensure only authorized keys for Azure storage encryption with desired assignment and rotation policy are assigned (e.g. using Azure Policy in deny mode). | Create a blob with unauthorized keys for Azure storage encryption, it should be denied. | Very Low | Storage.FC1 | Storage.T14 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C66]  Monitor the creation/update and usage keys for Azure storage encryption with desired assignment and rotation policy assignment (e.g. using monitoring logs on authentication type in AccountKey). | Configure a storage account with an unauthorized encryption settings, it should be detected. | Low | Storage.FC1 | Storage.T14 (Medium) | Medium |

## Apply cloud adoption, strategy, and governance [Storage.CO13]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C77]  Maintain a list of authorized Azure storage region options. | Request the list of authorized Azure storage region, its review process, and its review records. | Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C78, depends on Storage.C77, assured by Storage.C80]  Ensure authorized Azure storage region is set for authorized storage accounts. | Request 1) the mechanism ensuring only Azure storage authorized region for storage accounts are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC1 | Storage.T14 (Very Low) | Very Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C79, depends on Storage.C77]  Ensure only authorized Azure storage region is set for authorized storage accounts (e.g. using Azure Policy in deny mode). | Create a storage account with unauthorized Azure storage region, it should be denied. | Very Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C80]  Verify only authorized Azure storage region is set for authorized storage accounts (e.g. using Azure Policy on audit mode). | Create a storage account with unauthorized Azure storage region, it should be detected. | High | Storage.FC1 | - | Very Low |

## Govern Cross-Origin resource sharing [Storage.CO14]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C96]  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) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C97, depends on Storage.C96, assured by Storage.C99]  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) plan to move any older storage accounts | High | Storage.FC1 | Storage.T26 (Low) | Very Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C98, depends on Storage.C96]  Prevent unauthorized storage accounts to use CORS trusted origins and corresponding settings (e.g. using Azure Policy in deny mode). | Create a storage account with untrusted CORS settings, it should be denied. | High | Storage.FC1 | Storage.T26 (Very Low) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C99]  Verify only authorized CORS trusted origins and corresponding settings are configured (e.g. using Azure Policy on audit mode). | Create a storage account with untrusted CORS settings, it should be detected. | High | Storage.FC1 | - | Very Low |

## Scan input/output objects for malware [Storage.CO15]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Preventative (COSO)  Detect (NIST CSF) | [Storage.C114]  If the storage account is used as an input or the output of a process, scan the objects for malware (e.g. using VirusScan) | Inject a malware test file, it should be denied. | High | Storage.FC2 | Storage.T12 (Very High) | Medium |

# Compliance Mapping

*The Control Objectives are mapped to the* [*Secure Controls Framework*](https://www.securecontrolsframework.com/secure-controls-framework) *(SCF), provided under Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0). Compliance mappings are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.*

*You can change the displayed Compliance mappings by contacting* [*chatbot@trustoncloud.com*](mailto:chatbot@trustoncloud.com)*.*

# 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 the access to the IAM actions required to perform attacks using Azure IAM, following the IAM Operating Model and using the Azure IAM ThreatModel. | Request the list of authorized IAM principals that have the permissions required to launch attacks, its review process, and its review records. | Medium | Storage.FC1  Storage.FC10  Storage.FC2  Storage.FC4  Storage.FC6  Storage.FC7 | Storage.T1 (Medium)  Storage.T2 (Medium)  Storage.T4 (Medium)  Storage.T5 (Medium)  Storage.T6 (Medium)  Storage.T7 (Medium)  Storage.T8 (Medium)  Storage.T9 (Medium)  Storage.T12 (Medium)  Storage.T23 (High)  Storage.T24 (Medium)  Storage.T25 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C23]  Limit access to delete storage accounts, via Azure Policy and IAM. Do not ever delete a sensitive storage account (e.g. just delete all data) to make sure that storage account FQDN cannot be used as a source of attacks. | Try to delete storage account, it should be denied | Medium | Storage.FC2 | Storage.T5 (Very High) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C82, assured by Storage.C83]  Block the usage of storage account access key, whenever possible. | Try to connect using storage account access keys - Expected error "key based authentication is not permitted on this storage account", it should be denied. | Medium | Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | Storage.T1 (Very High)  Storage.T2 (Very High)  Storage.T3 (Very High)  Storage.T9 (Very Low)  Storage.T12 (Very High)  Storage.T16 (Very Low)  Storage.T17 (Low)  Storage.T27 (Low)  Storage.T28 (Low) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C83]  Verify only authorized authorization method set for authorized blob, file shares, queues, tables, DFS (e.g. using Azure Policy on audit mode). | Configure a blob, file share, queue, table, or DFS with an unauthorized authorization method, it should be detected. | High | Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C111]  Maintain a list of authorized storage and corresponding accounts locks. | Request the list of authorized storage accounts locks settings, its review process, and its review records. | Very Low | Storage.FC2 | Storage.T5 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C112, depends on Storage.C111, assured by Storage.C113]  Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized storage accounts have lock disabled. | Request 1) the mechanism ensuring only authorized storage accounts have locks disabled, 2) its records of execution for all new storage accounts locks, and 3) plan to move any older storage accounts | Very Low | Storage.FC2 | Storage.T5 (High) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C113]  Verify the creation/update of storage accounts lock and corresponding settings (e.g. using activity logs "localized Value": "Delete management locks"). | Delete a storage account lock, it should be detected. | Very Low | Storage.FC2 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C68]  Maintain a list of authorized encryption in transit methods with desired assignment to storage accounts. Ideally minimum TLS 1.2. | Request the list of authorized encryption in transit methods, its review process, and its review records. | Very Low | Storage.FC1  Storage.FC3 | Storage.T11 (Very Low)  Storage.T21 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C69, depends on Storage.C68, assured by Storage.C72]  Ensure authorized encryption in transit methods with desired assignment is set for authorized storage accounts. | Request 1) the mechanism ensuring only encryption in transit methods with desired assignment are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Low | Storage.FC1  Storage.FC3 | Storage.T11 (High)  Storage.T21 (Medium) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C70, depends on Storage.C68]  Ensure storage accounts have authorized encryption in transit methods configured (e.g. using Azure Policy in deny mode). | Create a blob with unauthorized encryption in transit methods for Azure storage, it should be denied. | Medium | Storage.FC1  Storage.FC3 | Storage.T11 (Very High)  Storage.T21 (Medium) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C72]  Verify only authorized encryption in transit methods with desired assignment is set for authorized storage accounts (e.g. using Azure Policy on audit mode). | Configure a storage account with an unauthorized encryption in transit settings, it should be detected. | Low | Storage.FC1  Storage.FC3 | - | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C28, depends on Storage.C27]  Ensure only authorized Groups are used in ACLs for data Lake storage Gen2. | Review ACLs against usage of individual users' service principal. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T30 (Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C33, depends on Storage.C32]  Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method. | Request the IAM operating model for the directories and objects. | Low | Storage.FC2  Storage.FC3 | Storage.T6 (Very Low)  Storage.T7 (High)  Storage.T9 (High)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C31, depends on Storage.C30]  Use immutable blobs. | Check the usage of immutable blobs. | Medium | Storage.FC2 | Storage.T8 (Very High)  Storage.T9 (Very High)  Storage.T12 (Medium) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C5, depends on Storage.C1]  Integrate the access to files and directories via ACL in the IAM Operating Model | Request the IAM operating model for the access to files and directories via ACL | Low | Storage.FC2  Storage.FC4 | Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C94, depends on Storage.C92]  Prevent unauthorized storage accounts to have the static website hosting option enabled (e.g. using Azure Policy on deny mode). | Create a storage account with a static website hosting option enabled, it should be denied. | Very Low | Storage.FC2 | Storage.T22 (Medium) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C58]  Maintain a list of authorized blob and containers with public access level set to anonymous, ideally none | Request the list of authorized blob and containers with public access level set to anonymous, its review process, and its review records. | Low | Storage.FC2 | Storage.T5 (Very Low)  Storage.T6 (Very Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C60, depends on Storage.C58]  Ensure only authorized blob and containers are anonymously accessed (e.g. using Azure Policy in deny mode). | Create a blob, or a container anonymously accessible, it should be denied. | Very Low | Storage.FC2 | Storage.T5 (Medium)  Storage.T6 (Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C40]  Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS access via private endpoint. | Request the list of authorized IPs, its review process, and its review records. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T6 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T12 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T30 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C41, depends on Storage.C40, assured by Storage.C43]  Ensure only authorized VNET are configured for the blob, file shares, queues, tables, DFS. | Request 1) the mechanism ensuring PE are in place 2) its records of execution for all new DFS. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T6 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Low)  Storage.T29 (Low)  Storage.T30 (Low)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C42, depends on Storage.C40]  Prevent the use of unauthorized VNETs by the storage account (e.g. by using Azure Policy). | Configure an unauthorized VNETs on a storage account, it should be denied. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T6 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T30 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C43]  Verify the unauthorized VNETs cannot access to the storage account. | Configure an unauthorized VNETs on a storage account, it should be detected. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | - | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C45]  Maintain a list of IPs authorized to access each storage account. | Request the list of authorized blobs to use allowblobPublicAccess enabled, its review process, and its review records. | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T30 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C46, depends on Storage.C45, assured by Storage.C48]  Ensure traffic is denied from all networks including trusted services, logging and metrics read access, and allow traffic only from authorized list ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | Request 1) the mechanism ensuring firewall rules are in place 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (High)  Storage.T3 (High)  Storage.T5 (High)  Storage.T6 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T30 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C48]  Verify access is possible only from allowed list (e.g. by using Azure Policy) | Connect to storage from not allowed IP, it should be detected. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | - | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C92]  Maintain a list of authorized storage accounts has static website hosting option enabled, ideally none | Request the list of authorized storage accounts with static website hosting option enabled, its review process, and its review records. | Low | Storage.FC2 | Storage.T22 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C30]  Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob. | Request the list of directories and blobs for immutable blobs functionality. | Medium | Storage.FC2 | Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C55, depends on Storage.C53]  Ensure storage accounts have diagnostic settings configured according to the design. | Create a storage account with on approved diagnostic settings options, it should be denied. | Very Low | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T10 (High)  Storage.T13 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C27]  Maintain a list of authorized Groups to use in permissions for data Lake storage Gen2. | Request the list of authorized Groups, its review process, and its review records. | Very Low | Storage.FC2  Storage.FC3 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C29, depends on Storage.C27]  Use name convention for Groups adding Suffix R/RW and Entity to be used. | Review Group-Name convention. | Medium | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T30 (Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C44]  Managed Identity is the preferred method for accessing data Lake storage Gen2 from parent services. | Check if underlying services are not using SAS, or other password methods to authenticate. | Medium | Storage.FC2  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T12 (High) | Medium |
| Corrective (COSO)  Protect (NIST CSF) | [Storage.C81]  Integrate the access to blob, file shares, queues, tables and DFS via SAS token in the IAM Operating Model, ideally prioritising AD as preferred method. | Check if (Azure) Active Directory is used for assigning permissions. | Medium | Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | Storage.T1 (Low)  Storage.T3 (Low)  Storage.T16 (Very Low)  Storage.T17 (Low)  Storage.T18 (Low)  Storage.T19 (Low)  Storage.T27 (Low)  Storage.T28 (Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C2]  Define an ACL or IAM authentication for every data Lake storage Gen2. Ideally use Azure AD only, and multiple DLS if fine-grained access is required. | Request the list of all storage accounts you control, define their authorized data classification, identify whether the data is primary and the mechanism and records to ensure the accuracy of those metadata | High | Storage.FC2  Storage.FC3 | Storage.T5 (Very Low)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C3, depends on Storage.C2]  Use a data discovery tool to control that no sensitive data are stored in unauthorized storage account | Upload a higher classification data in a storage account, it should be detected. | Medium | Storage.FC2 | Storage.T5 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C24]  Maintain a list of authorized IPs to use SAS tokens, and their authorized time window. | Request the list of authorized IPs to use SAS tokens, its review process, and its review records. | Very Low | Storage.FC4  Storage.FC7 | Storage.T3 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C25, depends on Storage.C24, assured by Storage.C26]  Ensure SAS tokens allow only authorized IPs, using the sourceIP field and enforcing HTTPS. | Request 1) the mechanism ensuring SAS tokens allow only authorized IPs, 2) its records of execution for all new SAS tokens, and 3) plan to move any older SAS tokens. | Very Low | Storage.FC2  Storage.FC4  Storage.FC7 | Storage.T1 (Low)  Storage.T3 (Low)  Storage.T9 (Very Low)  Storage.T12 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C26]  Verify SAS tokens only allow authorized IPs. | Deploy a SAS token with an unauthorized IP, it should be detected | Medium | Storage.FC2  Storage.FC4  Storage.FC7 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C6]  Maintain a list of authorized storage accounts with allowblobPublicAccess enabled, ideally none | Request the list of authorized storage accounts with allowblobPublicAccess enabled, its review process, and its review records. | Low | Storage.FC2 | Storage.T5 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C7, depends on Storage.C6, assured by Storage.C9]  Ensure no storage accounts have allowblobPublicAccess enabled, except if authorized. | Request 1) the mechanism ensuring only authorized storage accounts have allowblobPublicAccess enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2  Storage.FC3 | Storage.T5 (Medium)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C8, depends on Storage.C6]  Prevent the creation/update of storage accounts with allowblobPublicAccess enabled (e.g. using Azure Policy on deny mode - "[Preview]: storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be denied. | High | Storage.FC2  Storage.FC3 | Storage.T5 (Medium)  Storage.T6 (Medium)  Storage.T15 (Very Low)  Storage.T30 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C9]  Verify no storage accounts have allowblobPublicAccess enabled (e.g. using Azure Policy on audit mode - "[Preview]: storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be detected. | High | Storage.FC2  Storage.FC3 | - | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C52]  Verify storage accounts with cross-tenant replication enabled (e.g. using Azure Policy "storage accounts should prevent cross tenant object replication" in audit mode.). | Creation of storage account with cross-tenant option enabled, it should be detected. | Low | Storage.FC2  Storage.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C93, depends on Storage.C92, assured by Storage.C95]  Ensure only authorized storage accounts has the static website hosting option enabled. | Request 1) the mechanism ensuring only authorized storage accounts has static website hosting option enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2 | Storage.T22 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C95]  Verify only authorized storage accounts has the static website hosting option enabled (e.g. using Azure Policy on audit mode). | Create a storage account with a static website hosting option enabled, it should be detected. | High | Storage.FC2 | - | Medium |
| Directive (COSO)  Recover (NIST CSF) | [Storage.C12]  Backup primary data in a location which have different security authority ([ref 1](https://docs.microsoft.com/en-us/azure/backup/blob-backup-overview), [ref 2](https://docs.microsoft.com/en-us/azure/backup/backup-afs)) | Request the mechanism used to backup primary data in a location which have different security authority, its records of execution, and records of restoration testing | High | Storage.FC2  Storage.FC3 | Storage.T7 (High)  Storage.T17 (Low)  Storage.T18 (Medium)  Storage.T19 (Medium)  Storage.T20 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C49]  Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, DFS, including regular testing. | Request the backup policies for DFS, its review process, and its review records. | Low | Storage.FC2 | Storage.T7 (Medium)  Storage.T9 (Medium)  Storage.T12 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C50]  Maintain a list of objects with cross-tenant replication enabled. | Request the list of authorized objects use allow cross-tenant replication, its review process, and its review records. | Low | Storage.FC2  Storage.FC9 | Storage.T5 (Very Low)  Storage.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C51, depends on Storage.C50, assured by Storage.C52]  Ensure cross-tenant replication is allowed only for specific storage accounts. | Request 1) the mechanism ensuring allowblobPublicAccess allow only authorized blobs, 2) its records of execution for all new blobs. | High | Storage.FC2  Storage.FC9 | Storage.T5 (High)  Storage.T6 (High)  Storage.T13 (High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C13]  For each storage account (or type of data), define the minimum retention of container and blob from the deletion (e.g. 7 days) | For each storage account, request the minimum retention of container and blob from the deletion, its review process, and its review records | Low | Storage.FC2 | Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C15, depends on Storage.C13]  Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy in deny mode). | Create a storage account without soft-delete for the blob, it should be denied | High | Storage.FC2 | Storage.T9 (High) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C18, depends on Storage.C13]  Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode). | Create a storage account without soft-delete for the container, it should be denied. | High | Storage.FC2 | Storage.T9 (High) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C34, assured by Storage.C36]  Ensure storage accounts have soft-delete for the blob enabled | Request 1) the mechanism ensuring storage accounts have soft-delete for the blob enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2  Storage.FC6 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T25 (Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C35]  Prevent the creation of storage accounts without soft-delete for the blob option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode). | Create a storage account without soft-delete for the blob, it should be denied | High | Storage.FC2  Storage.FC6 | Storage.T9 (High)  Storage.T25 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C36]  Verify all storage accounts have soft-delete for the blob enabled | Create a storage account without soft-delete for the blob option, it should be detected. | Low | Storage.FC2  Storage.FC6 | - | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C38, depends on Storage.C34]  Prevent the creation of storage accounts without soft-delete for the container option (e.g. by using an Azure Policy in deny mode). | Create a storage account without soft-delete for the container, it should be denied. | High | Storage.FC2  Storage.FC6 | Storage.T9 (High)  Storage.T25 (Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C59, depends on Storage.C58, assured by Storage.C62]  Ensure anonymous access level is set only for authorized blobs / containers. | Request 1) the mechanism ensuring only authorized blob / container are anonymously accessed, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2 | Storage.T5 (Medium)  Storage.T6 (Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C61]  Monitor the creation/update of blob and containers that are anonymously accessed (e.g. using Azure Automations). | Create a blob, or a container anonymously accessible, it should be detected. | Low | Storage.FC2 | Storage.T5 (Medium)  Storage.T6 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C62]  Verify only authorized blob or containers are anonymously accessible (e.g. using Azure Policy on audit mode). | Create 1) a blob, or 2) a container anonymously accessible, it should be detected. | High | Storage.FC2 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C85]  For each file share, define the minimum retention of container and blob from the deletion (e.g. 7 days) | For each file share, request the minimum retention from the deletion, its review process, and its review records | High | Storage.FC3 | Storage.T18 (Very Low)  Storage.T19 (Very Low)  Storage.T20 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C86, depends on Storage.C85, assured by Storage.C88]  Ensure file shares have soft-delete enabled for at least the defined minimum retention | Request 1) the mechanism ensuring file shares have soft-delete enabled for at least the defined minimum retention, 2) it's records of execution for all new file shares, and 3) plan to move any older file shares | Low | Storage.FC3 | Storage.T18 (Medium)  Storage.T19 (Very Low)  Storage.T20 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C88]  Verify all file shares have soft-delete (e.g. by using an Azure Policy in audit mode). | Create a file share without soft-delete , it should be detected. | Low | Storage.FC3 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C108, assured by Storage.C110]  Ensure storage accounts have Azure Defender enabled | Request 1) the mechanism ensuring storage accounts have Azure Defender for storage account enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C110]  Verify storage accounts without Azure Defender for storage account enabled. | Create a storage account without Azure Defender for storage account, it should be detected. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C20]  Maintain a list of authorized storage accounts with hierarchical namespace (DFS) option enabled. | Request the list of authorized {resources}, its review process, and its review records | Medium | Storage.FC2 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C21, depends on Storage.C20, assured by Storage.C22]  Ensure only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured | Request 1) the mechanism ensuring only authorized storage accounts with hierarchical namespace (DFS) option enabled are configured, 2) its records of execution for all new storage accounts with hierarchical namespace (DFS) option enabled and 3) plan to move any older storage accounts with hierarchical namespace (DFS) option enabled. | Medium | Storage.FC2 | Storage.T6 (Low)  Storage.T7 (Low)  Storage.T30 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C22]  Verify storage accounts with hierarchical namespace (DFS) option enabled are not configured (e.g. by using an Azure Policy {"isHnsEnabled": "true"} in audit mode) | Create a storage account with hierarchical namespace (DFS) option enabled, it should be detected | Medium | Storage.FC2 | - | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C71]  Monitor the creation/update usage encryption in transit methods with desired assignment is set for authorized storage accounts (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly"). | Configure a storage account with an unauthorized encryption in transit settings, it should be detected. | Low | Storage.FC1  Storage.FC3 | Storage.T11 (Medium)  Storage.T21 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C47, depends on Storage.C45]  Prevent access from unauthorized IPs, by allowing only authorized IP using Azure Storage Firewall. | Access from unauthorized IPs, it should be denied. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T2 (Very Low)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T30 (Medium)  Storage.T31 (Low)  Storage.T32 (Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C53]  Define a diagnostic settings design for storage accounts including destination (tenant/subscription), categories (ideally all) and rotation, based on requirement. Resource logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs, Azure Event Hubs to forward outside of Azure, or to Azure storage for archiving. | Request the design of diagnostic settings for storage accounts, its review process, and its review records. | Low | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T10 (Very Low)  Storage.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C54, depends on Storage.C53, assured by Storage.C57]  Ensure diagnostic settings are configured properly to the architecture design. | Request 1) the mechanism ensuring only authorized diagnostic settings destinations are enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Low | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T10 (Medium)  Storage.T13 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C56]  Monitor the creation/update of storage accounts with diagnostic settings enabled (e.g. using activity logs on operation name - create or update resource diagnostic setting) | Configure a storage account with an unauthorized diagnostic settings options, it should be detected. | Low | Storage.FC8 | Storage.T10 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C57]  Verify storage accounts have diagnostic settings configured according to the design (e.g. using 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. | High | Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C63]  Maintain a list of authorized keys for Azure storage encryption with desired assignment and rotation policy. | Request the list of authorized keys for Azure storage encryption with desired assignment and rotation policy, its review process, and its review records. | Low | Storage.FC1 | Storage.T14 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C65, depends on Storage.C63]  Ensure only authorized keys for Azure storage encryption with desired assignment and rotation policy are assigned (e.g. using Azure Policy in deny mode). | Create a blob with unauthorized keys for Azure storage encryption, it should be denied. | Very Low | Storage.FC1 | Storage.T14 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C66]  Monitor the creation/update and usage keys for Azure storage encryption with desired assignment and rotation policy assignment (e.g. using monitoring logs on authentication type in AccountKey). | Configure a storage account with an unauthorized encryption settings, it should be detected. | Low | Storage.FC1 | Storage.T14 (Medium) | Medium |
| Preventative (COSO)  Detect (NIST CSF) | [Storage.C114]  If the storage account is used as an input or the output of a process, scan the objects for malware (e.g. using VirusScan) | Inject a malware test file, it should be denied. | High | Storage.FC2 | Storage.T12 (Very High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C89]  Maintain a revocation plan for any SAS or storage account access keys that you issue to clients based on requirements. If a SAS is compromised, you need to revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to quickly invalidate all signatures associated with that key. To revoke a service SAS that is associated with a stored access policy, you can delete the stored access policy, rename the policy, or change its expiry time to a time that is in the past ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas)). | Request the of authorized revocation plan for any SAS or storage account access keys, its review process, and its review records. | Low | Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C90, depends on Storage.C89, assured by Storage.C91]  Ensure the revocation plan is in place for any SAS or storage account access key. | Request 1) the mechanism ensuring revocation plan in place for any SAS or storage account access keys is in use, 2) its records of testing for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C91]  Verify the revocation plan is in place for any SAS or storage account access key. | Check test executions. Any unsuccessful attempts, it should be detected | High | Storage.FC3  Storage.FC7 | - | Low |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C4]  Use a data discovery tool to ensure the storage account names, object names, and tags do not contain sensitive data | Create 1) a storage account name, 2) object names, or 3) tags with sensitive data, it should be detected. | Very High | Storage.FC2 | Storage.T5 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C10, assured by Storage.C11]  Enable versioning on blobs holding primary data | Request the mechanism used to ensure versioning on blobs holding primary data, and its records | Medium | Storage.FC2 | Storage.T7 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C11]  Verify blobs holding primary data are versioned | Remove versioning from a blob holding primary data, it should be detected | High | Storage.FC2 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C73]  Maintain a list of authorized Azure storage redundancy options. | Request the list of authorized Azure storage redundancy, its review process, and its review records. | Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C75, depends on Storage.C73]  Ensure only authorized Azure storage redundancy is set for authorized storage accounts (e.g. using Azure Policy in deny mode). | Create a blob with unauthorized Azure storage redundancy for Azure storage, it should be denied. | Very Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C37, assured by Storage.C39]  Ensure storage accounts have soft-delete for the container enabled | Request 1) the mechanism ensuring storage accounts have soft-delete for the container enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC2  Storage.FC6 | Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T25 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C39]  Verify storage accounts without soft-delete for the container are not configured. | Create a storage account without soft-delete for the container option, it should be detected. | Low | Storage.FC2  Storage.FC6 | - | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C87, depends on Storage.C85]  Prevent the creation of file shares without soft-delete (e.g. by using an Azure Policy in deny mode). | Create a file share without soft-delete, it should be denied | High | Storage.FC3 | Storage.T18 (Medium)  Storage.T19 (Very Low)  Storage.T20 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C105, assured by Storage.C107]  Ensure storage accounts have Azure Defender for Storage account enabled" with "Ensure storage accounts have Azure Defender for storage account enabled | Request 1) the mechanism ensuring storage accounts have Azure Defender for storage account enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C106]  Prevent the creation of storage accounts without Azure Defender for storage account option (e.g. by using an Azure Policy "Microsoft.storage/storageaccounts/deleteRetentionPolicy" in deny mode). | Create a storage account without Azure Defender for storage account, it should be denied | High | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C107]  Verify all storage accounts have Azure Defender for storage account enabled | Create a storage account without Azure Defender for storage account option, it should be detected. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | - | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C109, depends on Storage.C105]  Prevent the creation of storage accounts without Azure Defender (e.g. by using an Azure Policy in deny mode). | Create a storage account without Azure Defender for storage account, it should be denied. | High | Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C67]  Verify only authorized keys for Azure storage encryption with desired assignment and rotation policy are in use (e.g. using Azure Policy on audit mode). | Configure a storage account with an unauthorized encryption settings, it should be detected. | High | Storage.FC1 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C100]  Maintain a list of authorized SMB 2.1 Azure Files. | Request the list of authorized SMB 2.1 Azure Files with SMB 2.1 settings, its review process, and its review records. | Low | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C101, depends on Storage.C100, assured by Storage.C104]  Ensure only authorized Azure Files SMB 2.1 have encryption disabled. | Request 1) the mechanism ensuring only authorized SMB 2.1 Azure Files have encryption disabled, 2) its records of execution for all new SMB 2.1 Azure Files, and 3) plan to move any older storage accounts | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C102, depends on Storage.C100]  Prevent unauthorized Azure Files SMB 2.1 to have encryption disabled (e.g. using Azure Policy in deny mode). | Create a storage account with encryption disabled, it should be denied. | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C103]  Monitor the creation/update of Azure Files SMB 2.1 and corresponding settings (e.g. using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly"). | Create a storage account with encryption disabled, it should be detected. | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C104]  Verify only authorized Azure Files SMB 2.1 and corresponding settings are configured (e.g. using Azure Policy on audit mode). | Create a storage account with encryption disabled, it should be detected. | High | Storage.FC3 | - | Low |
| Detective (COSO)  Protect (NIST CSF) | [Storage.C84]  Monitor file shares quotas and trends using Azure Monitor with alarm ([e.g. Azure file share size is 80% of capacity](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-monitoring?tabs=azure-portal#how-to-create-an-alert-if-the-azure-file-share-size-is-80-of-capacity)) | Create a file with unauthorized or default quota, it should be detected. | Very Low | Storage.FC3 | Storage.T16 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C64, depends on Storage.C63, assured by Storage.C67]  Ensure authorized keys for Azure storage encryption with desired assignment and rotation policy is set for authorized storage accounts. | Request 1) the mechanism ensuring only authorized keys for Azure storage encryption with desired assignment and rotation policy are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC1 | Storage.T14 (Medium) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C77]  Maintain a list of authorized Azure storage region options. | Request the list of authorized Azure storage region, its review process, and its review records. | Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C79, depends on Storage.C77]  Ensure only authorized Azure storage region is set for authorized storage accounts (e.g. using Azure Policy in deny mode). | Create a storage account with unauthorized Azure storage region, it should be denied. | Very Low | Storage.FC1 | Storage.T14 (Very Low) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C32]  Maintain an architecture of data Lake storage Gen2 ACL vs IAM based on requirements. Microsoft recommends using Azure Active Directory (Azure AD) to authorize requests against blob and queue data, if possible, instead of Shared Key. Azure AD provides superior security and ease of use over Shared Key. | Check documentation. | Medium | Storage.FC2 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T9 (Very Low) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C74, depends on Storage.C73, assured by Storage.C76]  Ensure authorized Azure storage redundancy is set for authorized storage accounts. | Request 1) the mechanism ensuring only Azure storage redundancy for storage accounts are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC1 | Storage.T14 (Very Low) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C76]  Verify only authorized Azure storage redundancy is set for authorized storage accounts (e.g. using Azure Policy on audit mode). | Configure a storage account with an unauthorized redundancy settings, it should be detected. | High | Storage.FC1 | - | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C14, depends on Storage.C13, assured by Storage.C16]  Ensure storage accounts have soft-delete for the blob enabled for at least the defined minimum retention | Request 1) the mechanism ensuring storage accounts have soft-delete for the blob enabled for at least the defined minimum retention, 2) its records of execution for all new storage accounts, and 3) 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.C16]  Verify all storage accounts have soft-delete for the blob enabled (e.g. by using an Azure Policy in audit mode). | Create a storage account without soft-delete for the blob option, it should be detected. | Low | Storage.FC2 | - | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C17, depends on Storage.C13, assured by Storage.C19]  Ensure storage accounts have soft-delete for the container enabled | Request 1) the mechanism ensuring storage accounts have soft-delete for the container enabled, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | Medium | Storage.FC2 | Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C19]  Verify storage accounts without soft-delete for the container are not configured. | Create a storage account without soft-delete for the container option, it should be detected. | Low | Storage.FC2 | - | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C78, depends on Storage.C77, assured by Storage.C80]  Ensure authorized Azure storage region is set for authorized storage accounts. | Request 1) the mechanism ensuring only Azure storage authorized region for storage accounts are in use, 2) its records of execution for all new storage accounts, and 3) plan to move any older storage accounts | High | Storage.FC1 | Storage.T14 (Very Low) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C80]  Verify only authorized Azure storage region is set for authorized storage accounts (e.g. using Azure Policy on audit mode). | Create a storage account with unauthorized Azure storage region, it should be detected. | High | Storage.FC1 | - | Very Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C96]  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) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C97, depends on Storage.C96, assured by Storage.C99]  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) plan to move any older storage accounts | High | Storage.FC1 | Storage.T26 (Low) | Very Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C98, depends on Storage.C96]  Prevent unauthorized storage accounts to use CORS trusted origins and corresponding settings (e.g. using Azure Policy in deny mode). | Create a storage account with untrusted CORS settings, it should be denied. | High | Storage.FC1 | Storage.T26 (Very Low) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C99]  Verify only authorized CORS trusted origins and corresponding settings are configured (e.g. using Azure Policy on audit mode). | Create a storage account with untrusted CORS settings, it should be detected. | High | Storage.FC1 | - | 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 | TODO | OperationsList |
| Storage.A2 | Notifies Azure Storage that virtual network or subnet is being deleted | Storage.FC1 | Microsoft.Storage/locations/deleteVirtualNetworkOrSubnets/action | TODO | NotifiesAzureStorageThatVirtualNetworkOrSubnetIsBeingDeleted |
| Storage.A3 | List blob services | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/read | TODO | Listblobs |
| Storage.A4 | Returns a user delegation key for the blob service | Storage.FC7 | Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action | TODO | ReturnsAUserDelegationKeyForTheblobService |
| Storage.A5 | Returns the result of put blob service properties | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/write | TODO | GetblobProperties |
| Storage.A6 | Returns blob service properties or statistics | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/read | TODO | SetblobServiceProperties |
| Storage.A7 | Returns a blob or a list of blobs | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read | TODO | Listblobs |
| Storage.A8 | Returns the result of writing a blob | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write | TODO | ReturnsTheResultOfWritingAblob |
| Storage.A9 | Returns the result of deleting a blob | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete | TODO | ReturnsTheResultOfDeletingAblob |
| Storage.A10 | Returns the result of deleting a blob version | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/deleteblobVersion/action | TODO | DeleteblobVersions |
| Storage.A11 | Delete a version of a blob. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/permanentDelete/action | TODO | DataactionForDeletingAVersionOfAblob |
| Storage.A12 | Returns the result of adding blob content | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action | TODO | AddblobContent |
| Storage.A13 | Returns the list of blobs under an account with matching tags filter | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action | TODO | ReturnsTheListOfblobsUnderAnAccountWithMatchingTagsFilter |
| Storage.A14 | Moves the blob from one path to another | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action | TODO | Moveblobs |
| Storage.A15 | Changes ownership of the blob | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/manageOwnership/action | TODO | ManageblobOwnership |
| Storage.A16 | Modifies permissions of the blob | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/modifyPermissions/action | TODO | ModifyblobPermissions |
| Storage.A17 | Returns the result of the blob command | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/runAsSuperUser/action | TODO | ReturnsTheResultOfTheblobCommand |
| Storage.A18 | Migrate | Storage.FC1 | Microsoft.Storage/storageAccounts/blobServices/containers/migrate/action | TODO | Migrate |
| Storage.A19 | Returns the result of patch blob container | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/write | TODO | PathblobContainer |
| Storage.A20 | Returns the result of deleting a container | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/delete | TODO | DeleteblobContainer |
| Storage.A21 | Returns a container | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/read | TODO | GetblobContainer |
| Storage.A22 | Returns list of containers | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/read | TODO | ReturnsListOfContainers |
| Storage.A23 | Returns the result of leasing blob container | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/lease/action | TODO | ReturnsTheResultOfLeasingblobContainer |
| Storage.A24 | Returns the result of put blob container | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/write | TODO | ReturnsTheResultOfPutblobContainer |
| Storage.A25 | Clear blob container legal hold | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/clearLegalHold/action | TODO | ClearblobContainerLegalHold |
| Storage.A26 | Set blob container legal hold | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/setLegalHold/action | TODO | SetblobContainerLegalHold |
| Storage.A27 | Extend blob container immutability policy | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/extend/action | TODO | ExtendblobContainerImmutabilityPolicy |
| Storage.A28 | Delete blob container immutability policy | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/delete | TODO | DeleteblobContainerImmutabilityPolicy |
| Storage.A29 | Put blob container immutability policy | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/write | TODO | PutblobContainerImmutabilityPolicy |
| Storage.A30 | Lock blob container immutability policy | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/lock/action | TODO | LockblobContainerImmutabilityPolicy |
| Storage.A31 | Get blob container immutability policy | Storage.FC6 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/read | TODO | GetblobContainerImmutabilityPolicy |
| Storage.A32 | Get queue service properties | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/read | TODO | GetqueueServiceProperties |
| Storage.A33 | Returns queue service properties or statistics. | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/read | TODO | ReturnsqueueServicePropertiesOrStatistics. |
| Storage.A34 | Returns the result of setting queue service properties | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/write | TODO | ReturnsTheResultOfSettingqueueServiceProperties |
| Storage.A35 | Create a queue | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/write | TODO | CreateAqueue |
| Storage.A36 | Returns a queue or a list of queues. | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/read | TODO | ReturnsAqueueOrAListOfqueues. |
| Storage.A37 | Returns the result of writing a queue | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/write | TODO | ReturnsTheResultOfWritingAqueue |
| Storage.A38 | Returns the result of deleting a queue | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/delete | TODO | ReturnsTheResultOfDeletingAqueue |
| Storage.A39 | Returns a message | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/messages/read | TODO | ReturnsAMessage |
| Storage.A40 | Returns the result of writing a message | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/messages/write | TODO | ReturnsTheResultOfWritingAMessage |
| Storage.A41 | Returns the result of deleting a message | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/messages/delete | TODO | ReturnsTheResultOfDeletingAMessage |
| Storage.A42 | Returns the result of adding a message | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/messages/add/action | TODO | ReturnsTheResultOfAddingAMessage |
| Storage.A43 | Returns the result of processing a message | Storage.FC4 | Microsoft.Storage/storageAccounts/queueServices/queues/messages/process/action | TODO | ReturnsTheResultOfProcessingAMessage |
| Storage.A44 | Update internal properties | Storage.FC1 | Microsoft.Storage/storageAccounts/updateInternalProperties/action | TODO | UpdateInternalProperties |
| Storage.A45 | Customer is able to abort an ongoing hierarchical namespace migration on the storage account | Storage.FC1 | Microsoft.Storage/storageAccounts/hnsonmigration/action | TODO | CustomerIsAbleToAbortAnOngoingHierarchicalNamespaceMigrationOnTheStorageAccount |
| Storage.A46 | Customer is able to migrate to hierarchical namespace account type | Storage.FC1 | Microsoft.Storage/storageAccounts/hnsonmigration/action | TODO | CustomerIsAbleToMigrateToHierarchicalNamespaceAccountType |
| Storage.A47 | Restore blob ranges to the state of the specified time | Storage.FC2 | Microsoft.Storage/storageAccounts/restoreblobRanges/action | TODO | RestoreblobRangesToTheStateOfTheSpecifiedTime |
| Storage.A48 | Approve private endpoint Connections | Storage.FC1 | Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action | TODO | ApprovePrivateEndpointConnections |
| Storage.A49 | Customer is able to control the failover in case of availability issues | Storage.FC1 | Microsoft.Storage/storageAccounts/failover/action | TODO | CustomerIsAbleToControlTheFailoverInCaseOfAvailabilityIssues |
| Storage.A50 | Returns the access keys for the specified storage account. | Storage.FC7 | Microsoft.Storage/storageAccounts/listkeys/action | TODO | ReturnsTheAccessKeysForTheSpecifiedStorageAccount. |
| Storage.A51 | Regenerates the access keys for the specified storage account. | Storage.FC7 | Microsoft.Storage/storageAccounts/regeneratekey/action | TODO | RegeneratesTheAccessKeysForTheSpecifiedStorageAccount. |
| Storage.A52 | Rotate key | Storage.FC7 | Microsoft.Storage/storageAccounts/rotateKey/action | TODO | RotateKey |
| Storage.A53 | Revokes all the user delegation keys for the specified storage account. | Storage.FC7 | Microsoft.Storage/storageAccounts/revokeUserDelegationKeys/action | TODO | RevokesAllTheUserDelegationKeysForTheSpecifiedStorageAccount. |
| Storage.A54 | Deletes an existing storage account. | Storage.FC1 | Microsoft.Storage/storageAccounts/delete | TODO | DeletesAnExistingStorageAccount. |
| Storage.A55 | Returns the list of storage accounts or gets the properties for the specified storage account. | Storage.FC1 | Microsoft.Storage/storageAccounts/read | TODO | ReturnsTheListOfStorageAccountsOrGetsThePropertiesForTheSpecifiedStorageAccount. |
| Storage.A56 | Returns the account SAS token for the specified storage account. | Storage.FC1 | Microsoft.Storage/storageAccounts/listAccountSas/action | TODO | ReturnsTheAccountSASTokenForTheSpecifiedStorageAccount. |
| Storage.A57 | Returns the service SAS token for the specified storage account. | Storage.FC1 | Microsoft.Storage/storageAccounts/listServiceSas/action | TODO | ReturnsTheServiceSASTokenForTheSpecifiedStorageAccount. |
| Storage.A58 | Creates a storage account with the specified parameters, updates the properties or tags, or adds a custom domain for the specified storage account. | Storage.FC1 | Microsoft.Storage/storageAccounts/write | TODO | CreatesAStorageAccountWithTheSpecifiedParametersOrUpdateThePropertiesOrTagsOrAddsCustomDomainForTheSpecifiedStorageAccount. |
| Storage.A59 | Create/update storage account diagnostic settings. | Storage.FC1 | Microsoft.Storage/storageAccounts/services/diagnosticsettings/write | TODO | Create/UpdateStorageAccountDiagnosticSettings. |
| Storage.A60 | Get list of Azure Storage metrics definitions. | Storage.FC8 | Microsoft.Storage/storageAccounts/providers/Microsoft.Insights/metricDefinitions/read | TODO | GetListOfAzureStorageMetricsDefinitions. |
| Storage.A61 | Gets the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/providers/Microsoft.Insights/diagnosticsettings/read | TODO | GetsTheDiagnosticSettingForTheResource. |
| Storage.A62 | Creates or updates the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/providers/Microsoft.Insights/diagnosticsettings/write | TODO | CreatesOrUpdatesTheDiagnosticSettingForTheResource. |
| Storage.A63 | Get list of Azure Storage metrics definitions. | Storage.FC8 | Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/metricDefinitions/read | TODO | GetListOfAzureStorageMetricsDefinitions. |
| Storage.A64 | Gets the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/diagnosticsettings/read | TODO | GetsTheDiagnosticSettingForTheResource. |
| Storage.A65 | Creates or updates the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/diagnosticsettings/write | TODO | CreatesOrUpdatesTheDiagnosticSettingForTheResource. |
| Storage.A66 | Get list of Azure Storage metrics definitions. | Storage.FC8 | Microsoft.Storage/storageAccounts/tableServices/providers/Microsoft.Insights/metricDefinitions/read | TODO | GetListOfAzureStorageMetricsDefinitions. |
| Storage.A67 | Gets the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/tableServices/providers/Microsoft.Insights/diagnosticsettings/read | TODO | GetsTheDiagnosticSettingForTheResource. |
| Storage.A68 | Creates or updates the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/tableServices/providers/Microsoft.Insights/diagnosticsettings/write | TODO | CreatesOrUpdatesTheDiagnosticSettingForTheResource. |
| Storage.A69 | Get list of Azure Storage metrics definitions. | Storage.FC8 | Microsoft.Storage/storageAccounts/fileServices/providers/Microsoft.Insights/metricDefinitions/read | TODO | GetListOfAzureStorageMetricsDefinitions. |
| Storage.A70 | Gets the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/fileServices/providers/Microsoft.Insights/diagnosticsettings/read | TODO | GetsTheDiagnosticSettingForTheResource. |
| Storage.A71 | Creates or updates the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/fileServices/providers/Microsoft.Insights/diagnosticsettings/write | TODO | CreatesOrUpdatesTheDiagnosticSettingForTheResource. |
| Storage.A72 | Get list of Azure Storage metrics definitions. | Storage.FC8 | Microsoft.Storage/storageAccounts/queueServices/providers/Microsoft.Insights/metricDefinitions/read | TODO | GetListOfAzureStorageMetricsDefinitions. |
| Storage.A73 | Gets the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/queueServices/providers/Microsoft.Insights/diagnosticsettings/read | TODO | GetsTheDiagnosticSettingForTheResource. |
| Storage.A74 | Creates or updates the diagnostic setting for the resource. | Storage.FC8 | Microsoft.Storage/storageAccounts/queueServices/providers/Microsoft.Insights/diagnosticsettings/write | TODO | CreatesOrUpdatesTheDiagnosticSettingForTheResource. |
| Storage.A75 | Gets the log definition for table | Storage.FC8 | Microsoft.Storage/storageAccounts/tableServices/providers/Microsoft.Insights/logDefinitions/read | TODO | GetsTheLogDefinitionForTable |
| Storage.A76 | Gets the log definition for blob | Storage.FC8 | Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/logDefinitions/read | TODO | GetsTheLogDefinitionForblob |
| Storage.A77 | Gets the log definition for file | Storage.FC8 | Microsoft.Storage/storageAccounts/fileServices/providers/Microsoft.Insights/logDefinitions/read | TODO | GetsTheLogDefinitionForFile |
| Storage.A78 | Gets the log definition for queue | Storage.FC8 | Microsoft.Storage/storageAccounts/queueServices/providers/Microsoft.Insights/logDefinitions/read | TODO | GetsTheLogDefinitionForqueue |
| Storage.A79 | Lists the SKUs supported by Azure Storage | Storage.FC1 | Microsoft.Storage/skus/read | TODO | ListsTheSkusSupportedByAzureStorage |
| Storage.A80 | Polls the status of an asynchronous operation | Storage.FC1 | Microsoft.Storage/operations/read | TODO | PollsTheStatusOfAnAsynchronousOperation |
| Storage.A81 | Checks that account name is valid and is not in use. | Storage.FC1 | Microsoft.Storage/checknameavailability/read | TODO | ChecksThatAccountNameIsValidAndIsNotInUse. |
| Storage.A82 | Returns the limit and the current usage count for resources in the specified subscription | Storage.FC1 | Microsoft.Storage/locations/usages/read | TODO | ReturnsTheLimitAndTheCurrentUsageCountForResourcesInTheSpecifiedSubscription |
| Storage.A83 | Returns the limit and the current usage count for resources in the specified subscription | Storage.FC1 | Microsoft.Storage/usages/read | TODO | ReturnsTheLimitAndTheCurrentUsageCountForResourcesInTheSpecifiedSubscription |
| Storage.A84 | Returns the result of reading blob tags | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/read | TODO | ReturnsTheResultOfReadingblobTags |
| Storage.A85 | Returns the result of writing blob tags | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write | TODO | ReturnsTheResultOfWritingblobTags |
| Storage.A86 | Delete storage account management policies | Storage.FC1 | Microsoft.Storage/storageAccounts/managementPolicies/delete | TODO | DeleteStorageAccountManagementPolicies |
| Storage.A87 | Get storage management account policies | Storage.FC1 | Microsoft.Storage/storageAccounts/managementPolicies/read | TODO | GetStorageManagementAccountPolicies |
| Storage.A88 | Put storage account management policies | Storage.FC1 | Microsoft.Storage/storageAccounts/managementPolicies/write | TODO | PutStorageAccountManagementPolicies |
| Storage.A89 | Restore file share | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/shares/action | TODO | RestoreFileShare |
| Storage.A90 | List file services | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/read | TODO | ListFileServices |
| Storage.A91 | Put file service properties | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/write | TODO | PutFileServiceProperties |
| Storage.A92 | Get file service properties | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/read | TODO | GetFileServiceProperties |
| Storage.A93 | Get table service properties | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/read | TODO | GetTableServiceProperties |
| Storage.A94 | Get table service properties or statistics | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/read | TODO | GetTableServicePropertiesOrStatistics |
| Storage.A95 | Set table service properties | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/write | TODO | SetTableServiceProperties |
| Storage.A96 | Returns a file/folder or a list of files/folders | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/fileshares/files/read | TODO | ReturnsAFile/FolderOrAListOfFiles/Folders |
| Storage.A97 | Returns the result of writing a file or creating a folder | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write | TODO | ReturnsTheResultOfWritingAFileOrCreatingAFolder |
| Storage.A98 | Returns the result of deleting a file/folder | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/fileshares/files/delete | TODO | ReturnsTheResultOfDeletingAFile/Folder |
| Storage.A99 | Returns the result of modifying permission on a file/folder | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/fileshares/files/modifypermissions/action | TODO | ReturnsTheResultOfModifyingPermissionOnAFile/Folder |
| Storage.A100 | Get file admin privileges | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/fileshares/files/actassuperuser/action | TODO | GetFileAdminPrivileges |
| Storage.A101 | Get private endpoint Connection Proxy | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/read | TODO | GetPrivateEndpointConnectionProxy |
| Storage.A102 | Delete private endpoint Connection Proxies | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/delete | TODO | DeletePrivateEndpointConnectionProxies |
| Storage.A103 | Put private endpoint Connection Proxies | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnectionProxies/write | TODO | PutPrivateEndpointConnectionProxies |
| Storage.A104 | List private endpoint Connections | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnections/read | TODO | ListPrivateEndpointConnections |
| Storage.A105 | Delete private endpoint Connection | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnections/delete | TODO | DeletePrivateEndpointConnection |
| Storage.A106 | Get private endpoint Connection | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnections/read | TODO | GetPrivateEndpointConnection |
| Storage.A107 | Put private endpoint Connection | Storage.FC1 | Microsoft.Storage/storageAccounts/privateEndpointConnections/write | TODO | PutPrivateEndpointConnection |
| Storage.A108 | Get StorageAccount groupids | Storage.FC1 | Microsoft.Storage/storageAccounts/privateLinkResources/read | TODO | GetStorageaccountGroupids |
| Storage.A109 | Checks that account name is valid and is not in use. | Storage.FC1 | Microsoft.Storage/locations/checknameavailability/read | TODO | ChecksThatAccountNameIsValidAndIsNotInUse. |
| Storage.A110 | Delete file share | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/shares/delete | TODO | DeleteFileShare |
| Storage.A111 | Get file share | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/shares/read | TODO | GetFileShare |
| Storage.A112 | List file shares | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/shares/read | TODO | ListFileShares |
| Storage.A113 | Create or update file share | Storage.FC3 | Microsoft.Storage/storageAccounts/fileServices/shares/write | TODO | CreateOrUpdateFileShare |
| Storage.A114 | Encryption | Storage.FC9 | Microsoft.Storage/storageAccounts/encryptionScopes/read | TODO | Encryption |
| Storage.A115 | Encryption | Storage.FC9 | Microsoft.Storage/storageAccounts/encryptionScopes/write | TODO | Encryption |
| Storage.A116 | Delete object replication policy | Storage.FC9 | Microsoft.Storage/storageAccounts/objectReplicationPolicies/delete | TODO | DeleteObjectReplicationPolicy |
| Storage.A117 | Get object replication policy | Storage.FC9 | Microsoft.Storage/storageAccounts/objectReplicationPolicies/read | TODO | GetObjectReplicationPolicy |
| Storage.A118 | List object replication policies | Storage.FC9 | Microsoft.Storage/storageAccounts/objectReplicationPolicies/read | TODO | ListObjectReplicationPolicies |
| Storage.A119 | Create or update object replication policy | Storage.FC9 | Microsoft.Storage/storageAccounts/objectReplicationPolicies/write | TODO | CreateOrUpdateObjectReplicationPolicy |
| Storage.A120 | Share policy | Storage.FC1 | Microsoft.Storage/storageAccounts/dataSharePolicies/delete | TODO | SharePolicy |
| Storage.A121 | Share policy | Storage.FC1 | Microsoft.Storage/storageAccounts/dataSharePolicies/read | TODO | SharePolicy |
| Storage.A122 | Share policy | Storage.FC1 | Microsoft.Storage/storageAccounts/dataSharePolicies/write | TODO | SharePolicy |
| Storage.A123 | Delete local user | Storage.FC1 | Microsoft.Storage/storageAccounts/localUsers/delete | TODO | DeleteLocalUser |
| Storage.A125 | List local user keys | Storage.FC7 | Microsoft.Storage/storageAccounts/localusers/listKeys/action | TODO | ListLocalUserKeys |
| Storage.A126 | List local users | Storage.FC1 | Microsoft.Storage/storageAccounts/localusers/read | TODO | ListLocalUsers |
| Storage.A127 | Get local user | Storage.FC1 | Microsoft.Storage/storageAccounts/localusers/read | TODO | GetLocalUser |
| Storage.A128 | Create or update local user | Storage.FC1 | Microsoft.Storage/storageAccounts/localusers/write | TODO | CreateOrUpdateLocalUser |
| Storage.A129 | Query tables | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/read | TODO | QueryTables |
| Storage.A130 | Create tables | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/write | TODO | CreateTables |
| Storage.A131 | Delete tables | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/delete | TODO | DeleteTables |
| Storage.A132 | Policies read | Storage.FC10 | Microsoft.Storage/storageAccounts/inventoryPolicies/delete | TODO | PoliciesRead |
| Storage.A134 | Policies write | Storage.FC10 | Microsoft.Storage/storageAccounts/inventoryPolicies/write | TODO | PoliciesWrite |
| Storage.A135 | Delete lock | Storage.FC1 | Microsoft.Storage/storageAccounts/accountLocks/deleteLock/action | TODO | DeleteLock |
| Storage.A136 | Lock read | Storage.FC1 | Microsoft.Storage/storageAccounts/accountLocks/read | TODO | LockRead |
| Storage.A137 | Lock write | Storage.FC1 | Microsoft.Storage/storageAccounts/accountLocks/write | TODO | LockWrite |
| Storage.A138 | Lock delete | Storage.FC1 | Microsoft.Storage/storageAccounts/accountLocks/delete | TODO | LockDelete |
| Storage.A139 | Data share policy read | Storage.FC1 | Microsoft.Storage/storageAccounts/consumerdataSharePolicies/read | TODO | DataSharePolicyRead |
| Storage.A140 | Data share policy write | Storage.FC1 | Microsoft.Storage/storageAccounts/consumerdataSharePolicies/write | TODO | DataSharePolicyWrite |
| Storage.A141 | Query table entities | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/entities/read | TODO | QueryTableEntities |
| Storage.A142 | Insert, merge, or replace table entities | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/entities/write | TODO | Insert  Merge  OrReplaceTableEntities |
| Storage.A143 | Delete table entities | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/entities/delete | TODO | DeleteTableEntities |
| Storage.A144 | Insert table entities | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/entities/add/action | TODO | InsertTableEntities |
| Storage.A145 | Merge or update table entities | Storage.FC5 | Microsoft.Storage/storageAccounts/tableServices/tables/entities/update/action | TODO | MergeOrUpdateTableEntities |
| Storage.A146 | Run as Super user | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/immutableStorage/runAsSuperUser/action | TODO | RunAsSuperUser |
| Storage.A147 | Point markers | Storage.FC1 | Microsoft.Storage/storageAccounts/objectReplicationPolicies/restorePointMarkers/write | TODO | PointMarkers |
| Storage.A148 | Restore point delete | Storage.FC1 | Microsoft.Storage/storageAccounts/restorePoints/delete | TODO | RestorePointDelete |
| Storage.A149 | Restore point read | Storage.FC1 | Microsoft.Storage/storageAccounts/restorePoints/read | TODO | RestorePointRead |
| Storage.A150 | Blob service read | Storage.FC1 | Microsoft.Storage/storageAccounts/restorePoints/read | TODO | blobServiceRead |
| Storage.A151 | Blob service write | Storage.FC1 | Microsoft.Storage/storageAccounts/accountMigrations/read | TODO | blobServiceWrite |
| Storage.A152 | Manage storage account migration to enable hierarchical namespace. | Storage.FC1 | Microsoft.Storage/storageAccounts/accountMigrations/write | TODO | ContainerRead |
| Storage.A153 | List filesystems and their properties in given account. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/read | TODO | Filesystem\_List |
| Storage.A154 | Create a filesystem rooted at the specified location. If the filesystem already exists, the operation fails. This operation does not support conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/write | TODO | Filesystem\_Create |
| Storage.A155 | Set properties for the filesystem. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write | TODO | Filesystem\_Setproperties |
| Storage.A156 | List filesystem paths and their properties. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read | TODO | Path\_List |
| Storage.A157 | Get all system and user-defined filesystem properties are specified in the response headers. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/read | TODO | Filesystem\_Getproperties |
| Storage.A158 | Marks the filesystem for deletion. When a filesystem is deleted, a filesystem with the same identifier cannot be created for at least 30 seconds. While the filesystem is being deleted, attempts to create a filesystem with the same identifier will fail with status code 409 (Conflict), with the service returning additional error information indicating that the filesystem is being deleted. Get all other operations, including operations on any files or directories within the filesystem, will fail with status code 404 while the filesystem is being deleted. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/delete | TODO | Filesystem\_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. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write | TODO | 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. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write | TODO | Path\_Update |
| Storage.A161 | Create and manage a lease to restrict write and delete access to the path. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write | TODO | Path\_Lease |
| Storage.A162 | Read the contents of a file. For read operations, range requests are supported. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read | TODO | Path\_Read |
| Storage.A163 | Get properties returns all system and user defined properties for a path. Get status returns all system defined properties for a path. Get Access Control List returns the access control list for a path. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read | TODO | Path\_Getproperties |
| Storage.A164 | Delete the file or directory. This operation supports conditional HTTP requests. | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete | TODO | Path\_Delete |