# ThreatModel for Azure Storage

### 

### Introduction

Read the blog: [The last Azure Storage security document that we'll ever need.](https://trustoncloud.com/the-last-azure-security-document-that-well-ever-need/)

### Content

This publication includes:

- overall data flow diagram of Azure Storage

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

- prioritized list of all threat scenarios

- list of all the control activities and testing procedures

- risk-based prioritized list of control implementation

### License Agreement

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 | | 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 downstream processes with malware [Storage.T12] | Privilege escalation by modifying File System ACL [Storage.T6] |  |  |  |  |  | Privilege escalation using storage account access key [Storage.T1] | DoS due to storage account access key regeneration [Storage.T2] |
|  |  | Distribute malicious files via file share [Storage.T20] | Privilege escalation by modifying file share ACL [Storage.T17] |  |  |  |  |  | Access data using storage account access key or SAS token / data leakage due to disclosed SAS token [Storage.T3] | Recursively delete DFS directories and their content [Storage.T7] |
|  |  | Exfiltrate files via the static website feature [Storage.T22] | Usage of outdated vulnerable protocols to access file shares [Storage.T21] |  |  |  |  |  | Distribute malicious data by using the storage account name [Storage.T4] | Unauthorized modification of data [Storage.T8] |
|  |  | Distribute non-common malicious files via storage account bypassing Defender for storage [Storage.T35] | Unauthorized data exposed by breaking CORS settings [Storage.T26] |  |  |  |  |  | Unauthorized data made public [Storage.T5] | Encrypt/overwrite files by ransomware in DFS/blob [Storage.T9] |
|  |  | Distribute standard malicious files via storage account bypassing Defender for storage [Storage.T36] | Privilege escalation by modifying queue ACL [Storage.T27] |  |  |  |  |  | Exfiltrate data using diagnostic settings [Storage.T10] | Denial of wallet through file upload to storage account [Storage.T16] |
|  |  | Disable diagnostic settings [Storage.T41] | 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] |
|  |  |  | Data loss due to disabling soft deletion [Storage.T39] |  |  |  |  |  | Unauthorized access to data via storage account replication [Storage.T13] | Encrypt files by ransomware in file shares [Storage.T19] |
|  |  |  | Data loss due to disabling the versioning [Storage.T40] |  |  |  |  |  | Unauthorized access to data by direct access to the physical disk [Storage.T14] | 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] | DoS on wallet by executing Azure Data Lake Storage query acceleration [Storage.T34] |
|  |  |  |  |  |  |  |  |  | Unauthorized access to a sensitive message [Storage.T32] | DoS by tampering with encryption at rest key [Storage.T38] |
|  |  |  |  |  |  |  |  |  | Modify permissions by adding, modify or removing tags [Storage.T33] | Affect data by removing replication [Storage.T42] |
|  |  |  |  |  |  |  |  |  | Exfiltrate data by brute force enumeration of items from the storage account [Storage.T37] | Bypassing of soft delete by moving blob to archive tier [Storage.T54] |
|  |  |  |  |  |  |  |  |  | Privilege escalation by misconfiguration of NFS endpoint or by modifying current network settings [Storage.T43] |  |
|  |  |  |  |  |  |  |  |  | Access to data using stolen SFTP local user credentials [Storage.T44] |  |
|  |  |  |  |  |  |  |  |  | Usage of outdated vulnerable libraries to access Azure Storage account [Storage.T45] |  |
|  |  |  |  |  |  |  |  |  | Use of classic Azure Storage account [Storage.T46] |  |
|  |  |  |  |  |  |  |  |  | Exfiltrate data by using compromised credentials [Storage.T47] |  |
|  |  |  |  |  |  |  |  |  | Information disclosure due to unencrypted blob storage [Storage.T49] |  |
|  |  |  |  |  |  |  |  |  | Access to storage account resources by modifying virtual network rules [Storage.T50] |  |
|  |  |  |  |  |  |  |  |  | Recon of storage environment via examination of diagnostic logs [Storage.T53] |  |
|  |  |  |  |  |  |  |  |  | Gain access to blob by renaming file [Storage.T55] |  |

## 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 governed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) v4.1 protocol. |
| Monitoring | subclass of Storage account | Storage insights provide 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. |
| 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 | Object storage solution for storing amounts of unstructured data (blobs), that are accessible via HTTP/S and optionally via the Network File System (NFS) v3 and SFTP protocols. |
| Object replication | subclass of Blob storage, containers, Data Lake Storage Gen2 | Object replication asynchronously copies block blobs between a source storage account and a destination account. When you configure object replication, you create a replication policy that specifies the source storage account and the destination account. |
| 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. |
| Blob storage SSH File Transfer Protocol (SFTP) | subclass of Blob storage, containers, Data Lake Storage Gen2 | Blob storage supports the SSH File Transfer Protocol (SFTP). This support lets you securely connect to blob storage via an SFTP endpoint, allowing you to use SFTP for file access, file transfer, and file management. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  Threat List  |  |  | | --- | --- | | **Name** | **CVSS** | | Exfiltrate data by using compromised credentials | [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) | | Use of classic Azure Storage account | [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) | | Usage of outdated vulnerable libraries to access Azure Storage account | [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) | | 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) | | Distribute malicious data by using the storage account name | [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) | | Distribute non-common malicious files via storage account bypassing Defender for storage | [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) | | DoS by tampering with encryption at rest key | [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) | | Infiltrate unauthorized files into storage container | [Medium (4.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/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) | | Unauthorized 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) | | Access to storage account resources by modifying virtual network rules | [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:L/I:N/A:N) | | Cross service exploit | [Low (2.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L) | |

#### Exfiltrate data by using compromised credentials

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T47 | | **Name** | Exfiltrate data by using compromised credentials | | **Description** | An attacker can use compromised but authorized credentials to download your 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: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**    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.    Use Managed Identity as the method for accessing Azure Storage services. | Very High | 5 | - | - |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very High | - | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs using Azure Storage firewall. | High | 2 | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    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.    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method.    Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key.    Ensure the revocation plan is in place for any SAS or storage account access key. | High | 4 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 1 | - |

#### Use of classic Azure Storage account

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T46 | | **Name** | Use of classic Azure Storage account | | **Description** | Azure classic Storage Accounts don't support capabilities such as Azure Storage firewall. An attacker can more easily leverage the lack of controls in an Azure Storage account to launch an attack and impact the confidentiality, integrity, and availability of data stored within the account. | | **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** | {  "UNIQUE": ["Microsoft.Storage/storageAccounts/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features.    Monitor for creation of classic Azure Storage accounts (e.g., using activity log Microsoft.Storage/storageAccounts/writeoperation in operationName.value where properties.requestbody contains either *\"kind\":\"Storage\"* or *"kind\":\"BlobStorage\"*).    Ensure Storage Accounts are created as StorageV2    Prevent the creation of Storage Accounts that are not StorageV2 (e.g.,by using an Azure Policy in deny mode). | Very High | 2 | 1 | 1 |
| **Enforce encryption-at-rest**    Maintain a list of blobs created before October 20, 2017 (ideally none).    Rewrite every blob created before October 20, 2017. You can force encryption to occur immediately by downloading and re-uploading the blob | Low | 2 | - | - |

#### Usage of outdated vulnerable libraries to access Azure Storage account

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T45 | | **Name** | Usage of outdated vulnerable libraries to access Azure Storage account | | **Description** | The blob and queue storage client libraries use AES to encrypt user data. It's possible to use client-side encryption v1, which is NOT RECOMMENDED due to a security vulnerability in the client library's implementation of CBC mode. An attacker can perform a padding oracle attack to decrypt the blob's contents. | | **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** | {  "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/queueServices/queues/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Enforce good coding practice**    The latest (or latest -1 with no security vulnerabilities) non-preview version of storage software libraries must be used for Storage Accounts. Running on older versions could mean you are not using the latest security classes. Usage of such old classes and types can make your application vulnerable. | Very Low | 1 | - | - |

#### 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 a man-in-the-middle attack (e.g., with a 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 the 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 and clients performing checks against the certificate exposed by 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 |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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 with a DDoS attack. If your application approaches or exceeds 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** |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs 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, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 1 | - |

#### Distribute malicious data by using the storage account name

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T4 | | **Name** | Distribute malicious data by using the storage account name | | **Description** | Azure Storage account names are globally unique. An attacker can take over an old or existing account name, delete one, and 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 | - | - |
| **Protect primary data against loss**    Maintain a list of authorized storage and corresponding account locks (e.g., to prevent deletions).    Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized Storage Accounts have the lock disabled.    Monitor for unauthorized storage account deletions (e.g., using activity log Microsoft.Storage/storageAccounts/delete operation in operationName.value).    Maintain a list of authorized storage account deletions. The process for creating this list should ensure the storage account is not in use. | Very High | 3 | - | 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, files, SFTP access, NFS). Moreover, this 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 | - | - |

#### Distribute non-common malicious files via storage account bypassing Defender for storage

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T35 | | **Name** | Distribute non-common malicious files via storage account bypassing Defender for storage | | **Description** | Microsoft Defender for storage uses hash reputation analysis to determine whether an uploaded file is suspicious. The threat protection tools don’t scan the uploaded files; instead, they analyze the telemetry generated from the blobs storage and files services. Defender for storage then compares newly uploaded files' hashes with known viruses, trojans, spyware, and ransomware. An attacker can modify a well-known payload with one byte, and it will be undetected with Defender for storage. | | **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** | {  "OR": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write", "directory:R;file:R", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    Periodically scan files with third-party virus scanners that don't only rely on hashes | Medium | 1 | - | - |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Low | 1 | - | - |

#### DoS by tampering with encryption at rest key

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T38 | | **Name** | DoS by tampering with encryption at rest key | | **Description** | Azure Key Vault in the same or another tenant is used to store the encryption keys. An attacker can make it unavailable (e.g., by changing access policies), take over, perform DoS, or launch an attack on the storage account. | | **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** | {  "OR": ["Microsoft.KeyVault/vaults/keys/write", "Microsoft.KeyVault/vaults/keys/delete", "Microsoft.KeyVault/vaults/delete", "Microsoft.KeyVault/vaults/write", "Microsoft.Storage/storageAccounts/encryptionScopes/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 | - | - |
| **Enforce encryption-at-rest**    Protect Key Vault store custom encryption keys using Key Vault ThreatModel. | Low | 1 | - | - |

#### Infiltrate unauthorized files into storage container

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T57 | | **Name** | Infiltrate unauthorized files into storage container | | **Description** | Some Azure Stroage APIs allow for copying a blob or file from a 3rd party storage account to a container where the attacker has write access. The copy operation is not done from the host the attacker is issuing the command from, but from the Azure Storage service itself. An attacker can leverage this capability to infiltrate data into an environment where they otherwise do not have external access. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0011](https://attack.mitre.org/tactics/TA0011) | | **CVSS** | [Medium (4.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N) | | **IAM Access** | {  "OR": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write", "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. | Very High | 1 | - | - |
| **Identify and ensure the protection all Storage Accounts hosting your data**    *Preview control* . Ensure Storage Accounts have allowedCopyScope set to either AAD or PrivateLink    *Preview control* . Prevent the creation of Storage Accounts with allowedCopyScope not set to either AAD or PrivateLink (e.g. by using an Azure Policy in deny/append mode)    *Preview control* . Monitor that Storage Accounts with allowedCopyScope set to null / not specified are not created (e.g. using activity logs on "Create/Update Storage Account" operation in ."properties"."requestbody") | Very High | 1 | 1 | 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 and return 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 from using CORS trusted origins and corresponding settings (e.g., using Azure Policy in deny mode). | Very Low | 2 | 1 | - |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T14 | | **Name** | Unauthorized access to data by direct access to the physical disk | | **Description** | Azure operates the storage of physical disks. An attacker (i.e., an Azure insider) can access 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 are 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 of keys for Azure Storage encryption with desired assignment and rotation policy assignment (e.g., using [monitoring](about:blank)) logs on authentication type in AccountKey). | High | 2 | 1 | 1 |
| **Apply cloud adoption, strategy, and governance**    Maintain a list of authorized Azure Storage regions.    Ensure the 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). | High | 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 | - |

#### Access to storage account resources by modifying virtual network rules

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T50 | | **Name** | Access to storage account resources by modifying virtual network rules | | **Description** | Administrators configure network rules to allow only requests originating from authorized subnets. An attacker can insert/modify the rules to gain access. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **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:L/I:N/A:N) | | **IAM Access** | {  "UNIQUE": ["Microsoft.Storage/storageAccounts/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs using Azure Storage firewall. | High | 2 | 1 | - |
| **Enable soft-delete on containers, blobs, and file shares**    Maintain a list of authorized blobs and containers with public access level set to anonymous; ideally, none    Ensure the 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 blobs and containers that are anonymously accessed (e.g., using Azure Automations). | High | 2 | 1 | 1 |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 1 | - |
| **Ensure no storage account allows public access to blobs**    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 - "Storage account public access should be disallowed"). | Low | 2 | 1 | - |

#### Cross service exploit

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T51 | | **Name** | Cross service exploit | | **Description** | An attacker can manipulate storage services to trigger a compute service like Azure functions, allowing an attacker to exploit further resources. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0011](https://attack.mitre.org/tactics/TA0011) | | **CVSS** | [Low (2.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L) | | **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**    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 monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 Storage Accounts have diagnostic settings configured according to the design. | Very High | 1 | 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** | | Regenerates the access keys for the specified storage account. | Microsoft.Storage/storageAccounts/regeneratekey/ac  tion |  Threat List  |  |  | | --- | --- | | **Name** | **CVSS** | | Access data using storage account access key or SAS token / data leakage due to disclosed 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 using storage account 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) | | DoS due to storage account access key regeneration | [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) | |

#### Access data using storage account access key or SAS token / data leakage due to disclosed SAS token

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T3 | | **Name** | Access data using storage account access key or SAS token / data leakage due to disclosed SAS token | | **Description** | Storage account access keys have unrestricted access to the storage account they are coming from; a SAS token can give access to a blob, directory, file, table, or queue. A developer could store the keys, access tokens, or SAS URLs in an insecure location, such as a public code repository or client-side code. An attacker can use a stolen storage account access key or SAS token/URL to access or maliciously modify 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: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** |
| **Enable monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 | 2 | 1 | - |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very High | - | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Govern the use of Shared Keys and SAS tokens**    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.    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method.    Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key.    Ensure the revocation plan is in place for any SAS or storage account access key. | High | 4 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 1 | - |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Use Managed Identity as the method for accessing Azure Storage services. | Very Low | 1 | - | - |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    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 using storage account access key

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T1 | | **Name** | Privilege escalation using storage account access key | | **Description** | Storage Accounts can have up to 2 storage access keys with unrestricted permissions on this storage account. An attacker can generate a new storage access key or use an existing key to gain unrestricted access (e.g., az storage blob delete --account-key xxx --account-name xxx -c xxx --name xxx). | | **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"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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.    Use Managed Identity as the method for accessing Azure Storage services. | Very High | 2 | - | - |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very High | - | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs 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, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method.    Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key.    Ensure the revocation plan is in place for any SAS or storage account access key. | Low | 2 | - | - |

#### DoS due to storage account access key regeneration

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T2 | | **Name** | DoS due to storage account access key regeneration | | **Description** | SAS tokens can be signed from a storage account access key. Enabling non-Azure applications to access data in a storage account. An attacker can rotate or regenerate a storage account access key to invalidate its SAS tokens 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"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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.    Use Managed Identity as the method for accessing Azure Storage services. | Very High | 2 | - | - |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible.    Monitor for unauthorized storage account access key rotations (e.g., using activity log Microsoft.Storage/storageAccounts/regenerateKey/action operation in operationName.value).    Maintain a list of authorized storage account access key rotations. | Very High | 1 | 1 | 1 |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method.    Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key.    Ensure the revocation plan is in place for any SAS or storage account access key. | Low | 2 | - | - |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| File shares *(subclass of Storage account, FC3)* *Azure Files offers fully governed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) v4.1 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 of outdated vulnerable 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) | | Encrypt files 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) | | Denial of wallet through file upload to storage account | [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 or NFS v4.1 protocols can be accessible using REST APIs with the HTTP/S protocol. An attacker can access data using a different access method to gain access to the data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](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** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/fileServices/fileshares/files/read"  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **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.    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 and TAG based.    Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | Very High | 6 | - | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs 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, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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 data**    Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Medium | 1 | - | - |
| **Restrict the use of Azure Blob Storage SFTP**    Do not mix the different services like Azure Files, SFTP, and NFS inside the same Azure Storage account. | Medium | 1 | - | - |

#### Usage of outdated vulnerable protocols to access file shares

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T21 | | **Name** | Usage of outdated vulnerable protocols to access file shares | | **Description** | Encryption in transit is often disabled to support a legacy application on an outdated operating system. An attacker can hack old protocols and libraries to gain more permissions ([attacks via SMB client](https://techcommunity.microsoft.com/t5/itops-talk-blog/how-to-defend-users-from-interception-attacks-via-smb-client/ba-p/1494995)). | | **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 the 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 and clients performing checks against the certificate exposed by 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 NFS/SMB 2.1 Azure Files.    Ensure only authorized Azure Files NFS/SMB 2.1 have encryption disabled.    Prevent unauthorized Azure Files NFS/SMB 2.1 from having encryption disabled (e.g., using Azure Policy in deny mode).    Monitor the creation/update of Azure Files NFS/SMB 2.1 and corresponding settings (e.g., using activity logs on properties.supportsHttpsTrafficOnly scope "supportsHttpsTrafficOnly").    Maintain a list of authorized Azure Files security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only).    Ensure authorized Azure Files options with security protocol settings are set for authorized Storage Accounts.    Ensure only authorized Azure Files options with security protocol settings are set for authorized Storage Accounts (e.g., using Azure Policy in deny mode utilizing "protocolSettings"/"smb"{"versions","authenticationMethods","kerberosTicketEncryption","channelEncryption":} fields).    Refrain from mixing or downgrading security options for the Azure Files shared inside the same Azure Storage account. | Very High | 7 | 3 | 2 |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Low | 1 | - | - |
| **Enforce good coding practice**    The latest (or latest -1 with no security vulnerabilities) non-preview version of storage software libraries must be used for Storage Accounts. Running on older versions could mean you are not using the latest security classes. Usage of such old classes and types can make your application vulnerable. | Very Low | 1 | - | - |

#### Privilege escalation by modifying file share ACL

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T17 | | **Name** | Privilege escalation by modifying file share ACL | | **Description** | File share ACLs limit access to entities via a file share endpoint. An attacker can modify those ACLs to escalate their 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** |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Low | - | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the 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)) | 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 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** |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    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).    Periodically scan files with third-party virus scanners that don't only rely on hashes    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 | 3 | 2 | - |
| **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 | - |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | 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)) | 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 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the 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 | - | - |

#### Encrypt files by ransomware in file shares

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T19 | | **Name** | Encrypt files by ransomware in file shares | | **Description** | An attacker can encrypt files, making them unusable in a 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 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the 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 | - | - |

#### Denial of wallet through file upload to storage account

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T16 | | **Name** | Denial of wallet through file upload to storage account | | **Description** | An attacker can upload terabytes to the storage account and cause billing implications - especially with the 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** | {  "OR": ["Microsoft.Storage/storageAccounts/fileServices/fileshares/files/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Enable monitoring & notifications for Storage Accounts**    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 |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very Low | - | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method.    Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key.    Ensure the revocation plan is in place for any SAS or storage account access key. | Very Low | 2 | - | - |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Monitoring *(subclass of Storage account, FC8)* *Storage insights provide 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** | | Disable diagnostic settings | [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) | | 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) | | Recon of storage environment via examination of diagnostic logs | [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) | |

#### Disable diagnostic settings

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T41 | | **Name** | Disable diagnostic settings | | **Description** | An attacker can disable diagnostic settings to hide their future actions. | | **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** | {  "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** |
| **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 monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 according to the design (e.g., using activity logs on operation name - create or update resource diagnostic setting) | Very High | 2 | 1 | 1 |

#### Exfiltrate data using diagnostic settings

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T10 | | **Name** | Exfiltrate data using diagnostic settings | | **Description** | Diagnostic settings can be set at the storage account and/or container 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 monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 according to the design (e.g., using activity logs on operation name - create or update resource diagnostic setting) | Very High | 2 | 1 | 1 |

#### Recon of storage environment via examination of diagnostic logs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T53 | | **Name** | Recon of storage environment via examination of diagnostic logs | | **Description** | An attacker can leverage the data present in the diagnostic logs (e.g., authorized IP addresses, resource URIs) as a means of mapping out the environment and dataflows to assist in further attacks. | | **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/read", "Microsoft.Storage/storageAccounts/providers/Microsoft.Insights/diagnosticsettings/read", "Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/diagnosticsettings/read", "Microsoft.Storage/storageAccounts/tableServices/providers/Microsoft.Insights/diagnosticsettings/read", "Microsoft.Storage/storageAccounts/fileServices/providers/Microsoft.Insights/diagnosticsettings/read", "Microsoft.Storage/storageAccounts/queueServices/providers/Microsoft.Insights/diagnosticsettings/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 monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 according to the design (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 limit access to entities via the queue share endpoint. An attacker can modify those ACLs to escalate their 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** |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Low | - | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method. | Low | - | - | - |

#### Unauthorized access to a sensitive message

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T32 | | **Name** | Unauthorized access to a sensitive message | | **Description** | An attacker can access the sensitive message or modify the message that other services will consume. | | **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/read", "Microsoft.Storage/storageAccounts/queueServices/queues/write", "Microsoft.Storage/storageAccounts/queueServices/write", "Microsoft.Storage/storageAccounts/queueServices/queues/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 | - | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs using Azure Storage firewall. | High | 2 | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    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. | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 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 | 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 be deleted with all the messages, and queue parameter changes can result in losing all the messages. An attacker can delete or alter the messages and queues using any 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 | - | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs using Azure Storage firewall. | High | 2 | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    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. | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 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 | Low | 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 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** |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Low | - | 1 | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method. | Low | - | - | - |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Blob storage, containers, Data Lake Storage Gen2 *(subclass of Storage account, FC2)* *Object storage solution for storing amounts of unstructured data (blobs), that are accessible via HTTP/S and optionally via the Network File System (NFS) v3 and SFTP protocols.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  |  |  | | --- | --- | | **Action** | **IAM Permission** | | 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** | | Gain access to blob by renaming file | [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) | | 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) | | Modify permissions by adding, modify or removing tags | [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) | | Exfiltrate data by brute force enumeration of items from the storage account | [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) | | Information disclosure due to unencrypted blob storage | [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) | | Privilege escalation by misconfiguration of NFS endpoint or by modifying current network settings | [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) | | Exfiltrate files via the static website feature | [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) | | Data loss due to disabling the versioning | [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) | | Data loss due to disabling soft deletion | [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 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) | | Encrypt/overwrite files 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 downstream processes with malware | [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) | | Unauthorized 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) | | Distribute standard malicious files via storage account bypassing Defender for storage | [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 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) | | Bypassing of soft delete by moving blob to archive tier | [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) | | DoS on wallet by executing Azure Data Lake Storage query acceleration | [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) | |

#### Gain access to blob by renaming file

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T55 | | **Name** | Gain access to blob by renaming file | | **Description** | When using blob path as a @resource attribute for a condition. An attacker can gain access to a blob by renaming a file. | | **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** | {  "UNIQUE": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Enable monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 according to the design (e.g., using activity logs on operation name - create or update resource diagnostic setting) | Very High | 2 | 1 | 1 |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very High | - | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 IPs 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, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | High | 2 | 1 | - |
| **Limit the IAM entities allowed to execute the IAM actions required to perform attacks**    Use Managed Identity as the method for accessing Azure Storage services. | Medium | 1 | - | - |
| **Govern the use of Shared Keys and SAS tokens**    Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method.    Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key.    Ensure the revocation plan is in place for any SAS or storage account access key. | Low | 2 | - | - |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    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 | - |

#### 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](https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/). | | **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", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/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.    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 ensure storage account FQDN cannot be used as a source of an attack. | Very High | 1 | 1 | - |
| **Enable monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 | 2 | 1 | - |
| **Protect primary data against loss**    Maintain a list of objects with cross-tenant or Storage Accounts without private endpoint replication (any storage account) enabled.    Ensure cross-tenant replication/any Storage Accounts are allowed only for specific Storage Accounts.    Maintain a list of authorized storage and corresponding account locks (e.g., to prevent deletions).    Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized Storage Accounts have the lock disabled. | Very High | 4 | - | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | High | 1 | - | - |
| **Enable soft-delete on containers, blobs, and file shares**    Maintain a list of authorized blobs and containers with public access level set to anonymous; ideally, none    Ensure the 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 blobs and containers that are anonymously accessed (e.g., using Azure Automations). | High | 2 | 1 | 1 |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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 data**    Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required.    Use a data discovery tool (e.g., Microsoft Purview) to control that no sensitive data is stored in an unauthorized storage account    Use a data discovery tool (e.g., Microsoft Purview) to ensure the storage account names, object names, and tags do not contain sensitive data | Medium | 1 | - | 2 |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    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). | Low | 2 | 2 | - |
| **Ensure no storage account allows public access to blobs**    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 - "Storage account public access should be disallowed"). | Low | 2 | 1 | - |

#### Modify permissions by adding, modify or removing tags

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T33 | | **Name** | Modify permissions by adding, modify or removing tags | | **Description** | Access to Azure Storage blobs can be configured based on tags and custom security attributes using attribute-based access control (ABAC) conditions. An attacker can modify the conditions and/or tags to escalate privileges, access data, or perform a DoS. | | **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** | {  "OR": ["microsoft.directory/attributeSets/allProperties/allTasks", "microsoft.directory/customSecurityAttributeDefinitions/allProperties/allTasks", "microsoft.directory/servicePrincipals/customSecurityAttributes/update", "microsoft.directory/users/customSecurityAttributes/update", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/storageAccounts/blobServices/write", "Microsoft.Storage/storageAccounts/blobServices/containers/write", "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 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 and TAG based.    Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | Very High | 4 | - | - |
| **Identify and ensure the protection all Storage Accounts hosting your data**    Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Medium | 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 Low | 1 | - | - |

#### Exfiltrate data by brute force enumeration of items from the storage account

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T37 | | **Name** | Exfiltrate data by brute force enumeration of items from the storage account | | **Description** | Even with the "Public read access for blobs only" property set, blobs can be accessed by adding the blob name to the URL to see the contents. An attacker can enumerate blobs using brute force and access them. | | **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**    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 monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 | 2 | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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 blobs and containers with public access level set to anonymous; ideally, none    Ensure the 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 blobs and containers that are anonymously accessed (e.g., using Azure Automations). | High | 2 | 1 | 1 |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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 data**    Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Medium | 1 | - | - |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    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). | Low | 2 | 2 | - |
| **Ensure no storage account allows public access to blobs**    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 - "Storage account public access should be disallowed"). | Low | 2 | 1 | - |

#### Information disclosure due to unencrypted blob storage

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T49 | | **Name** | Information disclosure due to unencrypted blob storage | | **Description** | A blob created before October 20, 2017, may not be encrypted and has to be rewritten to enforce encryption. An attacker can make use of this fact to get access to sensitive data. | | **Goal** | Launch another attack | | **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** | {} | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Enforce encryption-at-rest**    Maintain a list of blobs created before October 20, 2017 (ideally none).    Rewrite every blob created before October 20, 2017. You can force encryption to occur immediately by downloading and re-uploading the blob | High | 2 | - | - |
| **Apply cloud adoption, strategy, and governance**    Maintain a list of authorized Azure Storage regions.    Ensure the 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). | High | 2 | 1 | - |

#### Privilege escalation by misconfiguration of NFS endpoint or by modifying current network settings

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T43 | | **Name** | Privilege escalation by misconfiguration of NFS endpoint or by modifying current network settings | | **Description** | The only way to secure the NFS data in your account is by using a VNET and other network security settings. Any other tool used to secure data, including account key authorization, Azure Active Directory (AD) security, and Access Control Lists (ACLs), are not supported. An attacker can break the network rules and access the NFS files. | | **Goal** | Launch another attack | | **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** | {} | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 | 2 | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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, and DFS, including regular testing. | Medium | 1 | - | - |

#### Exfiltrate files via the static website feature

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T22 | | **Name** | Exfiltrate files via the static website feature | | **Description** | A storage account can be configured as a static website server. An attacker can distribute malicious and infected files via a website hosted on a storage account or exfiltrate data via this method. Note that disallowing blob public access for a storage account does not affect any static websites hosted in that storage account. The $web container is always publicly accessible. | | **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** |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized Storage Accounts that have the static website hosting option enabled; ideally, none | High | 1 | - | - |
| **Ensure no storage account allows public access to blobs**    Ensure only authorized Storage Accounts has the static website hosting option enabled.    Prevent unauthorized Storage Accounts from having the static website hosting option enabled (e.g., using Azure Policy on deny mode). | High | 1 | 1 | - |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Low | 1 | - | - |

#### Data loss due to disabling the versioning

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T40 | | **Name** | Data loss due to disabling the versioning | | **Description** | An attacker can first disable the versioning (especially by disabling soft deletion) to compromise the service. Disabling blob versioning does not delete existing blobs, versions, or snapshots. When you turn off blob versioning, any existing versions remain accessible in your storage account. No new versions are created. | | **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/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 | - | - |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Low | 1 | - | - |
| **Protect primary data against loss**    Enable versioning on blobs holding primary data    Enable snapshots to Azure Files holding primary data | Low | 2 | - | - |
| **Enable hierarchical namespace in storage account, only when required**    Maintain a list of authorized Storage Accounts with the hierarchical namespace (DFS) option enabled.    Ensure only authorized Storage Accounts with the hierarchical namespace (DFS) option enabled are configured | Low | 2 | - | - |

#### Data loss due to disabling soft deletion

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T39 | | **Name** | Data loss due to disabling soft deletion | | **Description** | An attacker can disable soft delete to compromise the service. If you disable blob soft delete, you can continue to access and recover soft-deleted objects in your storage account until the soft delete retention period has elapsed. | | **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/write", "Microsoft.Storage/storageAccounts/blobServices/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 | - | - |
| **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 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 | 4 | 3 | - |

#### Privilege escalation by modifying File System ACL

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T6 | | **Name** | Privilege escalation by modifying File System ACL | | **Description** | Filesystem ACLs limit access to entities via the filesystem endpoint (DFS). An attacker can modify those ACLs to escalate their 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/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/runAsSuperUser/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.    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 and TAG based.    Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | Very High | 5 | - | - |
| **Enable hierarchical namespace in storage account, only when required**    Maintain a list of authorized Storage Accounts with the hierarchical namespace (DFS) option enabled.    Ensure only authorized Storage Accounts with the hierarchical namespace (DFS) option enabled are configured | Low | 2 | - | - |

#### Encrypt/overwrite files by ransomware in DFS/blob

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T9 | | **Name** | Encrypt/overwrite files by ransomware in DFS/blob | | **Description** | An attacker can encrypt/overwrite files/objects in DFS or blobs using an encryption key under their control and request a ransom to access the decryption key. | | **Goal** | Direct Financial Gain | | **MITRE ATT&CK®** | [TA0040](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.    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 and TAG based.    Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | Very High | 7 | - | - |
| **Enable monitoring & notifications for Storage Accounts**    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. 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 data**    Use immutable blobs with proper policy. | Very High | 1 | - | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **Govern the use of Shared Keys and SAS tokens**    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. | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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, and 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 | - |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very Low | - | 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 Low | 1 | - | - |

#### Infect downstream processes with malware

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T12 | | **Name** | Infect downstream processes with malware | | **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 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.    Use Managed Identity as the method for accessing Azure Storage services. | Very High | 2 | - | - |
| **Enable monitoring & notifications for Storage Accounts**    Maintain a list of directories and blobs that do not need modification after uploading to DFS/blob. | Very High | 1 | - | - |
| **Restrict the use of Shared Key authorization**    Block the usage of the storage account access key whenever possible. | Very High | - | 1 | - |
| **Restrict access to the endpoints (where possible disable public endpoint)**    Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account    Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([ref](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-powershell)). | High | 2 | - | - |
| **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 | - |
| **Govern the use of Shared Keys and SAS tokens**    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. | High | 2 | - | - |
| **Connect via private endpoint**    Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a private endpoint.    Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP.    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 data**    Use immutable blobs with proper policy. | Medium | 1 | - | - |
| **Protect primary data against loss**    Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, and 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 | - | - |

#### Unauthorized modification of data

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T8 | | **Name** | Unauthorized modification of data | | **Description** | An attacker can modify data that can cause independent inconsistency subsystems. For example, a typical scenario for Data Lake Storage Gen2 is that data should not be modified after being uploaded to blob storage. | | **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** | {  "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **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 monitoring & notifications for Storage Accounts**    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. 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 data**    Use immutable blobs with proper policy. | Very High | 1 | - | - |

#### Distribute standard malicious files via storage account bypassing Defender for storage

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T36 | | **Name** | Distribute standard malicious files via storage account bypassing Defender for storage | | **Description** | Microsoft Defender for storage uses hash reputation analysis to determine whether an uploaded file is suspicious. An attacker can use the put block and put block list method where the telemetry doesn't contain a hash value. As a result, some operations can't be monitored for known malware uploads and, in that way, distribute the viruses. | | **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/blobServices/containers/blobs/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview**    Periodically scan files with third-party virus scanners that don't only rely on hashes | Medium | 1 | - | - |
| **Use StorageV2 accounts only**    Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Low | 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 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** | {  "OR": ["Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete", "Microsoft.Storage/storageAccounts/blobServices/containers/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 and TAG based.    Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | Very High | 7 | - | - |
| **Enable monitoring & notifications for Storage Accounts**    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. 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    Enable snapshots to Azure Files 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, and DFS, including regular testing. | Medium | 4 | - | - |
| **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 the hierarchical namespace (DFS) option enabled.    Ensure only authorized Storage Accounts with the hierarchical namespace (DFS) option enabled are configured | Low | 2 | - | - |

#### Bypassing of soft delete by moving blob to archive tier

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T54 | | **Name** | Bypassing of soft delete by moving blob to archive tier | | **Description** | Blob soft delete doesn't afford to overwrite protection for blobs in the archive tier. If a blob in the archive tier is deleted and overwritten with a new blob in any tier, then the overwritten blob is permanently deleted. An attacker can move the data to the archive tier and overwrite the data. | | **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** | {  "OR": ["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. | Very High | 1 | - | - |
| **Identify and ensure the protection all Storage Accounts hosting your data**    Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Medium | 1 | - | - |

#### DoS on wallet by executing Azure Data Lake Storage query acceleration

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T34 | | **Name** | DoS on wallet by executing Azure Data Lake Storage query acceleration | | **Description** | Query acceleration is used for data processing applications and can be executed on a storage account. Due to the increased compute load within the Azure Data Lake Storage service, the pricing model for using query acceleration differs from the normal Azure Data Lake Storage transaction model. An attacker can execute the queries and generate costs. | | **Goal** | Direct Financial Gain | | **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/blobServices/containers/blobs/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.    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. | Very High | 5 | - | - |
| **Identify and ensure the protection all Storage Accounts hosting your data**    Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Medium | 1 | - | - |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Object replication *(subclass of Blob storage, containers, Data Lake Storage Gen2, FC9)* *Object replication asynchronously copies block blobs between a source storage account and a destination account. When you configure object replication, you create a replication policy that specifies the source storage account and the destination account.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  |  |  | | --- | --- | | **Action** | **IAM Permission** | | Create or update object replication policy | Microsoft.Storage/storageAccounts/objectReplicatio  nPolicies/write |  Threat List  |  |  | | --- | --- | | **Name** | **CVSS** | | Unauthorized 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) | | Affect data by removing replication | [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 access to data via storage account replication

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T13 | | **Name** | Unauthorized access to data via storage account replication | | **Description** | Replication allows you to replicate objects and their metadata. Currently, it is not available for DFS, but that may be an additional attack vector in the future. An attacker can configure replication on a storage account to replicate objects (or its metadata or tagging) to exfiltrate data, e.g., using replication to a storage account publicly available. Additionally, replication to an unauthorized region may cause regulatory or compliance issues. | | **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** |
| **Enable monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 | 2 | 1 | - |
| **Apply cloud adoption, strategy, and governance**    Maintain a list of authorized Azure Storage regions.    Ensure the 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). | High | 2 | 1 | - |
| **Protect primary data against loss**    Maintain a list of objects with cross-tenant or Storage Accounts without private endpoint replication (any storage account) enabled.    Ensure cross-tenant replication/any Storage Accounts are allowed only for specific Storage Accounts. | Medium | 2 | - | - |

#### Affect data by removing replication

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T42 | | **Name** | Affect data by removing replication | | **Description** | Replication is a level of integrity protection and backup. An attacker can remove replication to affect data protection. | | **Goal** | Data manipulation | | **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/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 | - | - |
| **Enable monitoring & notifications for Storage Accounts**    Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 | 2 | 1 | - |
| **Protect primary data against loss**    Maintain a list of objects with cross-tenant or Storage Accounts without private endpoint replication (any storage account) enabled.    Ensure cross-tenant replication/any Storage Accounts are allowed only for specific Storage Accounts. | Medium | 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 create/modify and access blob inventory, get knowledge about running services, and exfiltrate metadata. | | **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** | | Put storage account management policies | Microsoft.Storage/storageAccounts/managementPolici  es/write |  Threat List  |  |  | | --- | --- | | **Name** | **CVSS** | | 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) | |

#### Delete data using Blob Storage lifecycle management

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T25 | | **Name** | Delete data using Blob Storage lifecycle management | | **Description** | An attacker can create/modify Blob Storage lifecycle management and delete data or impact data latency. | | **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** | {  "UNIQUE": "Microsoft.Storage/storageAccounts/managementPolicies/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 | - | - |
| **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 | - |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Blob storage SSH File Transfer Protocol (SFTP) *(subclass of Blob storage, containers, Data Lake Storage Gen2, FC11)* *Blob storage supports the SSH File Transfer Protocol (SFTP). This support lets you securely connect to blob storage via an SFTP endpoint, allowing you to use SFTP for file access, file transfer, and file management.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  |  |  | | --- | --- | | **Action** | **IAM Permission** | | Create or update local user | Microsoft.Storage/storageAccounts/localusers/write |  Threat List  |  |  | | --- | --- | | **Name** | **CVSS** | | Access to data using stolen SFTP local user credentials | [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) | |

#### Access to data using stolen SFTP local user credentials

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Threat Id** | Storage.T44 | | **Name** | Access to data using stolen SFTP local user credentials | | **Description** | An attacker can exfiltrate/manipulate data using stolen SFTP local user credentials. | | **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** | {  "UNIQUE": ["Microsoft.Storage/storageAccounts/localusers/write"]  } | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| **Directive** | **Preventative** | **Detective** |
| **Restrict the use of Azure Blob Storage SFTP**    Maintain a list of authorized Azure Storage SFTP options with authentication methods and permission models.    Ensure authorized Azure Storage SFTP options with authentication methods and permission models are set for authorized Storage Accounts.    Ensure only authorized Azure Storage SFTP options with authentication methods and permission models are set for authorized Storage Accounts (e.g., using Azure Policy in deny mode). | Low | 2 | 1 | - |
| **Manage Azure Storage local users**    Integrate the access to SSH in the IAM Operating Model, including monitoring of creating local SSH users.    Use SSH private key credentials for authentication as the preferred authentication method. | Very Low | 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 with 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.FC8  Storage.FC9 | 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)  Storage.T33 (Medium)  Storage.T34 (Medium)  Storage.T37 (Medium)  Storage.T38 (Medium)  Storage.T39 (Medium)  Storage.T40 (Medium)  Storage.T41 (Medium)  Storage.T42 (Medium)  Storage.T43 (Very Low)  Storage.T47 (Medium)  Storage.T51 (Very Low)  Storage.T53 (Medium)  Storage.T54 (Medium)  Storage.T57 (Low) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C25]  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 ensure storage account FQDN cannot be used as a source of an attack. | Try to delete a storage account, it should be denied | Medium | Storage.FC2 | Storage.T5 (Very High) | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C29]  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.FC1  Storage.FC2  Storage.FC3 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T15 (Very Low)  Storage.T34 (Very Low)  Storage.T47 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C30, depends on Storage.C29]  Ensure only authorized Groups are used in ACLs for Data Lake Storage Gen2. | Review ACLs against usage of individual users' service principal. | Low | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T34 (Very Low)  Storage.T47 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C31, depends on Storage.C29]  Use name convention for Groups adding Suffix R/RW and Entity to be used. | Review Group-Name convention. | Medium | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T34 (Very Low)  Storage.T47 (Very Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C34]  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.FC3 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T15 (Very Low)  Storage.T33 (Very Low)  Storage.T34 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C35, depends on Storage.C34]  Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method and TAG based. | 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.T33 (Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C36, depends on Storage.C35]  Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | 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.T33 (Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C47]  Use Managed Identity as the method for accessing Azure Storage services. | Check if underlying services are not using SAS or other password methods to authenticate. | Medium | Storage.FC1  Storage.FC2  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T12 (High)  Storage.T47 (Medium)  Storage.T55 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C87]  Verify only the authorized authorization method set for authorized blob, file shares, queues, tables, and 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.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | - | Very High |

## Identify and ensure the protection all Storage Accounts hosting your data [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 storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Request the list of all Storage Accounts you control, define their authorized data classification, and 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.T33 (Very Low)  Storage.T34 (Very Low)  Storage.T37 (Very Low)  Storage.T54 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C3, depends on Storage.C2]  Use a data discovery tool (e.g., Microsoft Purview) to control that no sensitive data is stored in an 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 (e.g., Microsoft Purview) 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.C33, depends on Storage.C32]  Use immutable blobs with proper policy. | Ask for immutable policies. 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.C144, assured by Storage.C147]  *Preview control* . Ensure Storage Accounts have allowedCopyScope set to either AAD or PrivateLink | Request 1) the mechanism ensuring only authorized Storage Accounts are configured, 2) its records of execution for all new Storage Accounts, and 3) the plan to update unauthorized Storage Accounts | High | Storage.FC1 | Storage.T57 (Medium) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C145]  *Preview control* . Prevent the creation of Storage Accounts with allowedCopyScope not set to either AAD or PrivateLink (e.g. by using an Azure Policy in deny/append mode) | Create a storage account with allowedCopyScope not specified (defaults to null), it should be denied | Low | Storage.FC1 | Storage.T57 (Very High) | High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C146]  *Preview control* . Monitor that Storage Accounts with allowedCopyScope set to null / not specified are not created (e.g. using activity logs on "Create/Update Storage Account" operation in ."properties"."requestbody") | Create a storage account with allowedCopyScope set to null, it should be detected | Low | Storage.FC1 | Storage.T57 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C147]  *Preview control* . Verify Storage Accounts with allowedCopyScope set to null, are not configured (e.g. by using an Azure Policy in audit mode) | Create a storage account with allowedCopyScope set to null, it should be detected | Medium | Storage.FC1 | - | Low |

## 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 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)  Storage.T33 (Very Low) | High |

## Ensure no storage account allows public access to blobs [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.FC1  Storage.FC2 | Storage.T5 (Very Low)  Storage.T37 (Very Low)  Storage.T50 (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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (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 - "Storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be denied. | High | Storage.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (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 - "Storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be detected. | High | Storage.FC1  Storage.FC2 | - | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C55]  Verify Storage Accounts with cross-tenant replication enabled/any Storage Accounts (e.g., using Azure Policy "Storage Accounts should prevent cross tenant object replication" / "allowedCopyScope" parameter in audit mode.). | Create a storage account with cross-tenant/any storage account option enabled, it should be detected. | Low | Storage.FC2  Storage.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C97, depends on Storage.C96, assured by Storage.C99]  Ensure only authorized Storage Accounts has the static website hosting option enabled. | Request 1) the mechanism ensuring only authorized Storage Accounts have the 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.C98, depends on Storage.C96]  Prevent unauthorized Storage Accounts from having 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.C99]  Verify only authorized Storage Accounts have 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)  Storage.T40 (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)  Protect (NIST CSF) | [Storage.C12, assured by Storage.C13]  Enable snapshots to Azure Files holding primary data | Request the mechanism used to ensure snapshots to Azure Files on blobs holding primary data and its records | Medium | Storage.FC2 | Storage.T7 (Low)  Storage.T40 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C13]  Verify Azure Files have snapshots configured as an alternative to the versioning. | Remove snapshots from an Azure Files account holding primary data, it should be detected | High | Storage.FC2 | - | Low |
| Directive (COSO)  Recover (NIST CSF) | [Storage.C14]  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.C52]  Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, and 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)  Storage.T43 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C53]  Maintain a list of objects with cross-tenant or Storage Accounts without private endpoint replication (any storage account) enabled. | Request the list of authorized objects used to allow cross-tenant replication/any Storage Accounts, its review process, and its review records. | Low | Storage.FC2  Storage.FC9 | Storage.T5 (Very Low)  Storage.T13 (Very Low)  Storage.T42 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C54, depends on Storage.C53, assured by Storage.C55]  Ensure cross-tenant replication/any Storage Accounts are allowed only for specific Storage Accounts. | Request 1) the mechanism ensuring any replication allows only authorized Storage Accounts, 2) its records of execution for all new blobs. | High | Storage.FC2  Storage.FC9 | Storage.T5 (High)  Storage.T13 (High)  Storage.T42 (High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C77]  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.C78, depends on Storage.C77, assured by Storage.C80]  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.C79, depends on Storage.C77]  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.C80]  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 setting, it should be detected. | High | Storage.FC1 | - | Very Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C116]  Maintain a list of authorized storage and corresponding account locks (e.g., to prevent deletions). | Request the list of authorized Storage Accounts locks settings, its review process, and its review records. | Very Low | Storage.FC1  Storage.FC2 | Storage.T4 (Very Low)  Storage.T5 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C117, depends on Storage.C116, assured by Storage.C118]  Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized Storage Accounts have the 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.FC1  Storage.FC2 | Storage.T4 (High)  Storage.T5 (High) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C118]  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.FC1  Storage.FC2 | - | Very High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C138, depends on Storage.C139]  Monitor for unauthorized storage account deletions (e.g., using activity log Microsoft.Storage/storageAccounts/delete operation in operationName.value). | Delete a storage account, it should be detected | Medium | Storage.FC1 | Storage.T4 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C139]  Maintain a list of authorized storage account deletions. The process for creating this list should ensure the storage account is not in use. | Request the list of authorized storage account deletions, its review process, and its review records. | Low | Storage.FC1 | Storage.T4 (Very Low) | Medium |

## 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.C15]  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)  Storage.T39 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C16, depends on Storage.C15, assured by Storage.C18]  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.C17, depends on Storage.C15]  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.C18]  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.C19, depends on Storage.C15, assured by Storage.C21]  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)  Storage.T39 (Very Low) | Very Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C20, depends on Storage.C15]  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)  Storage.T39 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C21]  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.C37, assured by Storage.C39]  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.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T25 (Low)  Storage.T39 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C38]  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)  Storage.T39 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C39]  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.C40, assured by Storage.C42]  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)  Storage.T39 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C41, depends on Storage.C37]  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)  Storage.T39 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C42]  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.C61]  Maintain a list of authorized blobs and containers with public access level set to anonymous; ideally, none | Request the list of authorized blobs and containers with public access level set to anonymous, its review process, and its review records. | Low | Storage.FC1  Storage.FC2 | Storage.T5 (Very Low)  Storage.T37 (Very Low)  Storage.T50 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C62, depends on Storage.C61, assured by Storage.C65]  Ensure the 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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C63, depends on Storage.C61]  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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (Very Low) | High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C64]  Monitor the creation/update of blobs 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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C65]  Verify only authorized blobs 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.FC1  Storage.FC2 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C89]  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.C90, depends on Storage.C89, assured by Storage.C92]  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) its 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.C91, depends on Storage.C89]  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.C92]  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 |

## 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.C22]  Maintain a list of authorized Storage Accounts with the 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.T40 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C23, depends on Storage.C22, assured by Storage.C24]  Ensure only authorized Storage Accounts with the 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 the hierarchical namespace (DFS) option enabled. | Medium | Storage.FC2 | Storage.T6 (Low)  Storage.T7 (Low)  Storage.T40 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C24]  Verify Storage Accounts with the 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 the hierarchical namespace (DFS) option enabled, it should be detected | Medium | Storage.FC2 | - | Low |

## 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.C71]  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 setting, it should be detected. | High | Storage.FC1 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C72]  Maintain a list of authorized encryption in transit methods with the 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.C73, depends on Storage.C72, assured by Storage.C76]  Ensure authorized encryption in transit methods with desired assignment is set for authorized Storage Accounts and clients performing checks against the certificate exposed by Storage Accounts. | Request 1) the mechanism ensuring only encryption in transit methods with the desired assignment is 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.C74, depends on Storage.C72]  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.C75]  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 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.C76]  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 unauthorized encryption in transit settings, it should be detected. | Low | Storage.FC1  Storage.FC3 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C104]  Maintain a list of authorized NFS/SMB 2.1 Azure Files. | Request the list of authorized NFS/SMB 2.1 Azure Files with NFS/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.C105, depends on Storage.C104, assured by Storage.C108]  Ensure only authorized Azure Files NFS/SMB 2.1 have encryption disabled. | Request 1) the mechanism ensuring only authorized NFS/SMB 2.1 Azure Files have encryption disabled, 2) its records of execution for all new NFS/SMB 2.1 Azure Files, and 3) a plan to move any older Storage Accounts | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C106, depends on Storage.C104]  Prevent unauthorized Azure Files NFS/SMB 2.1 from having 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.C107]  Monitor the creation/update of Azure Files NFS/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.C108]  Verify only authorized Azure Files NFS/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 |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C129]  Maintain a list of authorized Azure Files security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only). | Request the list of authorized Azure Files security protocol settings, its review process, and its review records. | Low | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C130, depends on Storage.C129, assured by Storage.C132]  Ensure authorized Azure Files options with security protocol settings are set for authorized Storage Accounts. | Request 1) the mechanism ensuring only Azure Files security protocol settings for Storage Accounts are in use, 2) its records of execution for all new Storage Accounts, and 3) the plan to move any older Storage Accounts. | High | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C131]  Ensure only authorized Azure Files options with security protocol settings are set for authorized Storage Accounts (e.g., using Azure Policy in deny mode utilizing "protocolSettings"/"smb"{"versions","authenticationMethods","kerberosTicketEncryption","channelEncryption":} fields). | Create a file with unauthorized Azure Files security protocol settings for Azure Storage, it should be denied. | Very Low | Storage.FC3 | Storage.T21 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C132]  Verify only authorized Azure Files options with security protocol options are set for authorized Storage Accounts (e.g., using Azure Policy on audit mode utilizing "protocolSettings"/"smb"{"versions","authenticationMethods","kerberosTicketEncryption","channelEncryption":} fields). | Configure a storage account with an unauthorized Azure Files security protocol settings model, it should be detected. | High | Storage.FC3 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C133]  Refrain from mixing or downgrading security options for the Azure Files shared inside the same Azure Storage account. | Check the configuration of Storage Accounts (Azure Files). | Medium | Storage.FC3 | Storage.T21 (Very Low) | 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.C43]  Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a 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.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T12 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low)  Storage.T37 (Very Low)  Storage.T43 (Very Low)  Storage.T47 (Very Low)  Storage.T50 (Very Low)  Storage.T55 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C44, depends on Storage.C43, assured by Storage.C46]  Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP. | Request 1) the mechanism ensuring PE is in place 2) its records of execution for all new DFS. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Low)  Storage.T29 (Low)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T37 (Low)  Storage.T43 (Very Low)  Storage.T47 (Very High)  Storage.T50 (Very Low)  Storage.T55 (Very High) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C45, depends on Storage.C43]  Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | Configure an unauthorized VNET on a storage account, it should be denied. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T37 (Low)  Storage.T43 (Very Low)  Storage.T47 (Very High)  Storage.T50 (Low)  Storage.T55 (Very High) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C46]  Verify the unauthorized VNETs cannot access the storage account. | Configure an unauthorized VNET on a storage account, it should be detected. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | - | High |

## Restrict access to the endpoints (where possible disable public endpoint) [Storage.CO10]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C48]  Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account | Request the list of authorized IP or resource instance rules, its review process, and its review records. | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T12 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low)  Storage.T37 (Very Low)  Storage.T43 (Very Low)  Storage.T47 (Very Low)  Storage.T50 (Very Low)  Storage.T55 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C49, depends on Storage.C48, assured by Storage.C51]  Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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.T1 (High)  Storage.T3 (High)  Storage.T5 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T37 (High)  Storage.T43 (Very Low)  Storage.T47 (High)  Storage.T50 (Low)  Storage.T55 (High) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C50, depends on Storage.C48]  Prevent access from unauthorized IPs by allowing only authorized IPs using Azure Storage firewall. | Access from unauthorized IPs, it should be denied. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very Low)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T47 (Very Low)  Storage.T50 (Low)  Storage.T55 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C51]  Verify access is possible only from the 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.C96]  Maintain a list of authorized Storage Accounts that have the static website hosting option enabled; ideally, none | Request the list of authorized Storage Accounts with the static website hosting option enabled, its review process, and its review records. | Low | Storage.FC2 | Storage.T22 (Very Low) | High |

## Enable monitoring & notifications for Storage Accounts [Storage.CO11]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C32]  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.C56]  Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 their review records. | Low | Storage.FC1  Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | 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)  Storage.T37 (Very Low)  Storage.T41 (Very Low)  Storage.T42 (Very Low)  Storage.T43 (Very Low)  Storage.T51 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C57, depends on Storage.C56, assured by Storage.C60]  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.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)  Storage.T37 (Very Low)  Storage.T41 (Very Low)  Storage.T42 (Very Low)  Storage.T43 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C58, depends on Storage.C56]  Ensure Storage Accounts have diagnostic settings configured according to the design. | Create a storage account with unauhorized diagnostic settings options, it should be denied. | Very Low | Storage.FC1  Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | 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)  Storage.T37 (Very Low)  Storage.T41 (Very Low)  Storage.T42 (Very Low)  Storage.T43 (Very Low)  Storage.T51 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C59]  Monitor the creation/update of Storage Accounts with diagnostic settings enabled according to the design (e.g., using activity logs on operation name - create or update resource diagnostic setting) | Configure a storage account with unauthorized diagnostic settings options, it should be detected. | Low | Storage.FC2  Storage.FC8 | Storage.T10 (Medium)  Storage.T41 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C60]  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.C88]  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 an 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.C66]  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.C67, depends on Storage.C66, assured by Storage.C71]  Ensure authorized keys for Azure Storage encryption with desired assignment and rotation policy are 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) the plan to move any older Storage Accounts | High | Storage.FC1 | Storage.T14 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C68]  Protect Key Vault store custom encryption keys using Key Vault ThreatModel. | Check settings for Key Vault. | High | Storage.FC1 | Storage.T38 (Medium) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C69, depends on Storage.C66]  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.C70]  Monitor the creation/update and usage of keys for Azure Storage encryption with desired assignment and rotation policy assignment (e.g., using [monitoring](about:blank)) logs on authentication type in AccountKey). | Configure a storage account with an unauthorized encryption setting, it should be detected. | Low | Storage.FC1 | Storage.T14 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C134]  Maintain a list of blobs created before October 20, 2017 (ideally none). | Request 1) the list of blobs created before October 20, 20017, 2) its records of execution for rewriting, and 3) the plan to rewriting. | Low | Storage.FC1  Storage.FC2 | Storage.T46 (Very Low)  Storage.T49 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C135]  Rewrite every blob created before October 20, 2017. You can force encryption to occur immediately by downloading and re-uploading the blob | Check the creation date. | High | Storage.FC1  Storage.FC2 | Storage.T46 (Medium)  Storage.T49 (Very High) | High |

## 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.C81]  Maintain a list of authorized Azure Storage regions. | Request the list of authorized Azure Storage regions, its review process, and its review records. | Low | Storage.FC1  Storage.FC2  Storage.FC9 | Storage.T13 (Very Low)  Storage.T14 (Very Low)  Storage.T49 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C82, depends on Storage.C81, assured by Storage.C84]  Ensure the authorized Azure Storage region is set for authorized Storage Accounts. | Request 1) the mechanism ensuring only Azure Storage authorized regions 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.FC2  Storage.FC9 | Storage.T13 (Very Low)  Storage.T14 (Very Low)  Storage.T49 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C83, depends on Storage.C81]  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.FC2  Storage.FC9 | Storage.T13 (Medium)  Storage.T14 (Very Low)  Storage.T49 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C84]  Verify only the authorized Azure Storage region is set for authorized Storage Accounts (e.g., using Azure Policy on audit mode). | Create a storage account with an unauthorized Azure Storage region, it should be detected. | High | Storage.FC1  Storage.FC2  Storage.FC9 | - | 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.C100]  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.C101, depends on Storage.C100, assured by Storage.C103]  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.C102, depends on Storage.C100]  Prevent unauthorized Storage Accounts from using 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.C103]  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.C119]  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 |

## Manage Azure Storage local users [Storage.CO16]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C121]  Integrate the access to SSH in the IAM Operating Model, including monitoring of creating local SSH users. | Request the IAM Operating Model for SSH access. | Low | Storage.FC11 | Storage.T44 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C122]  Use SSH private key credentials for authentication as the preferred authentication method. | Check the usage of local passwords in SFTP-enabled accounts. | Medium | Storage.FC11 | Storage.T44 (Very Low) | Low |

## Monitor Storage Accounts with Azure Defender for Storage and Mirosoft Purview [Storage.CO17]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C109, assured by Storage.C111]  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.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low)  Storage.T37 (Very Low)  Storage.T55 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C110]  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.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium)  Storage.T37 (Very Low)  Storage.T55 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C111]  Verify all Storage Accounts have Azure Defender for storage account enabled | Create a storage account without Azure Defender for storage, it should be detected. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C112]  Periodically scan files with third-party virus scanners that don't only rely on hashes | Request 1) the mechanism ensuring Storage Accounts have been scanned by a third-party tool and 2) its records of execution for all Storage Accounts. | Medium | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T20 (Medium)  Storage.T35 (Medium)  Storage.T36 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C113, assured by Storage.C115]  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.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium)  Storage.T37 (Low)  Storage.T55 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C114, depends on Storage.C109]  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.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low)  Storage.T37 (Very Low)  Storage.T55 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C115]  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 |

## Use StorageV2 accounts only [Storage.CO18]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C128]  Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Request 1) the mechanism ensuring only authorized Storage Accounts have been deployed using ASM model, 2) its records of execution for all new Storage Accounts, and 3) the plan to move any older Storage Accounts | Very Low | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T5 (Medium)  Storage.T20 (Very Low)  Storage.T21 (Very Low)  Storage.T22 (Very Low)  Storage.T35 (Very Low)  Storage.T36 (Very Low)  Storage.T40 (Very Low)  Storage.T46 (Very High) | Very High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C140]  Monitor for creation of classic Azure Storage accounts (e.g., using activity log Microsoft.Storage/storageAccounts/writeoperation in operationName.value where properties.requestbody contains either *\"kind\":\"Storage\"* or *"kind\":\"BlobStorage\"*). | Create a BlobStorage and Storagev1 account type, it should be detected. | Medium | Storage.FC1 | Storage.T46 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C141, assured by Storage.C143]  Ensure Storage Accounts are created as StorageV2 | 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.FC1 | Storage.T46 (Very Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C142, depends on Storage.C141]  Prevent the creation of Storage Accounts that are not StorageV2 (e.g.,by using an Azure Policy in deny mode). | Create a storage account type of BlobStorage or Storagev1, it should be denied. | High | Storage.FC1 | Storage.T46 (Very High) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C143]  Verify all Storage Accounts are of account kind StorageV2 | Create a storage account type of BlobStorage or Storagev1, it should be detected. | Low | Storage.FC1 | - | High |

## Restrict the use of Shared Key authorization [Storage.CO19]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C86, assured by Storage.C87]  Block the usage of the 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.FC1  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)  Storage.T47 (Very High)  Storage.T55 (Very High) | Very High |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C136, depends on Storage.C137]  Monitor for unauthorized storage account access key rotations (e.g., using activity log Microsoft.Storage/storageAccounts/regenerateKey/action operation in operationName.value). | Rotate a storage account access key, it should be detected | Medium | Storage.FC7 | Storage.T2 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C137]  Maintain a list of authorized storage account access key rotations. | Request the list of authorized storage account access key rotations, its review process, and its review records. | Low | Storage.FC7 | Storage.T2 (Very Low) | Medium |

## Enforce good coding practice [Storage.CO20]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C127]  The latest (or latest -1 with no security vulnerabilities) non-preview version of storage software libraries must be used for Storage Accounts. Running on older versions could mean you are not using the latest security classes. Usage of such old classes and types can make your application vulnerable. | Check the software libraries that are in use for Storage Accounts. | Very High | Storage.FC1  Storage.FC3 | Storage.T21 (Low)  Storage.T45 (Medium) | Low |

## Restrict the use of Azure Blob Storage SFTP [Storage.CO21]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C120]  Maintain a list of authorized Azure Storage SFTP options with authentication methods and permission models. | Request the list of authorized Azure Storage SFTP options with encryption settings, authentication methods, and permission model, its review process, and its review records. | Low | Storage.FC11 | Storage.T44 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C123, depends on Storage.C120, assured by Storage.C125]  Ensure authorized Azure Storage SFTP options with authentication methods and permission models are set for authorized Storage Accounts. | Request 1) the mechanism ensuring only Azure Storage SFTP options with encryption settings, authentication methods, and permission model for Storage Accounts are in use, 2) its records of execution for all new Storage Accounts, and 3) the plan to move any older Storage Accounts. | High | Storage.FC11 | Storage.T44 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C124, depends on Storage.C120]  Ensure only authorized Azure Storage SFTP options with authentication methods and permission models are set for authorized Storage Accounts (e.g., using Azure Policy in deny mode). | Create a blob with unauthorized Azure Storage SFTP options, encryption settings, authentication methods, and permission model for Azure Storage, it should be denied. | Very Low | Storage.FC11 | Storage.T44 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C125]  Verify only authorized Azure Storage SFTP options with authentication methodsand permission models are set for authorized Storage Accounts (e.g., using Azure Policy on audit mode). | Configure a storage account with unauthorized SFTP options, encryption settings, authentication methods, and permission models, it should be detected. | High | Storage.FC11 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C126]  Do not mix the different services like Azure Files, SFTP, and NFS inside the same Azure Storage account. | Check the configuration of Storage Accounts. | Medium | Storage.FC3 | Storage.T15 (Medium) | Medium |

## Govern the use of Shared Keys and SAS tokens [Storage.CO22]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C26]  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.FC1  Storage.FC2  Storage.FC4  Storage.FC7 | Storage.T3 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low)  Storage.T47 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C27, depends on Storage.C26, assured by Storage.C28]  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.FC1  Storage.FC2  Storage.FC4  Storage.FC7 | Storage.T3 (Low)  Storage.T9 (Very Low)  Storage.T12 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T47 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C28]  Verify SAS tokens only allow authorized IPs. | Deploy a SAS token with an unauthorized IP, it should be detected | Medium | Storage.FC1  Storage.FC2  Storage.FC4  Storage.FC7 | - | Medium |
| Corrective (COSO)  Protect (NIST CSF) | [Storage.C85]  Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method. | Check if (Azure) Active Directory is used for assigning permissions. | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | Storage.T1 (Low)  Storage.T2 (Low)  Storage.T3 (Low)  Storage.T16 (Very Low)  Storage.T17 (Low)  Storage.T18 (Low)  Storage.T19 (Low)  Storage.T27 (Low)  Storage.T28 (Low)  Storage.T47 (Low)  Storage.T55 (Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C93]  Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key. | Request the authorized revocation plan for any SAS or storage account access keys, its review process, and its review records. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low)  Storage.T47 (Very Low)  Storage.T55 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C94, depends on Storage.C93, assured by Storage.C95]  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.FC1  Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low)  Storage.T47 (Very Low)  Storage.T55 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C95]  Verify the revocation plan is in place for any SAS or storage account access key. | Check test executions. For any unsuccessful attempts, it should be detected | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC7 | - | Low |

# 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 with 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.FC8  Storage.FC9 | 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)  Storage.T33 (Medium)  Storage.T34 (Medium)  Storage.T37 (Medium)  Storage.T38 (Medium)  Storage.T39 (Medium)  Storage.T40 (Medium)  Storage.T41 (Medium)  Storage.T42 (Medium)  Storage.T43 (Very Low)  Storage.T47 (Medium)  Storage.T51 (Very Low)  Storage.T53 (Medium)  Storage.T54 (Medium)  Storage.T57 (Low) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C25]  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 ensure storage account FQDN cannot be used as a source of an attack. | Try to delete a storage account, it should be denied | Medium | Storage.FC2 | Storage.T5 (Very High) | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C29]  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.FC1  Storage.FC2  Storage.FC3 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T8 (Very Low)  Storage.T9 (Very Low)  Storage.T15 (Very Low)  Storage.T34 (Very Low)  Storage.T47 (Very Low) | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C34]  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.FC3 | Storage.T6 (Very Low)  Storage.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T15 (Very Low)  Storage.T33 (Very Low)  Storage.T34 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C35, depends on Storage.C34]  Integrate the access to directories and objects via ACL in the IAM Operating Model, not mixing IAM and ACL access method and TAG based. | 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.T33 (Low) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C87]  Verify only the authorized authorization method set for authorized blob, file shares, queues, tables, and 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.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C116]  Maintain a list of authorized storage and corresponding account locks (e.g., to prevent deletions). | Request the list of authorized Storage Accounts locks settings, its review process, and its review records. | Very Low | Storage.FC1  Storage.FC2 | Storage.T4 (Very Low)  Storage.T5 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C117, depends on Storage.C116, assured by Storage.C118]  Lock storage account to prevent accidental or malicious deletion or configuration changes and ensure only authorized Storage Accounts have the 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.FC1  Storage.FC2 | Storage.T4 (High)  Storage.T5 (High) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C118]  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.FC1  Storage.FC2 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C72]  Maintain a list of authorized encryption in transit methods with the 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.C73, depends on Storage.C72, assured by Storage.C76]  Ensure authorized encryption in transit methods with desired assignment is set for authorized Storage Accounts and clients performing checks against the certificate exposed by Storage Accounts. | Request 1) the mechanism ensuring only encryption in transit methods with the desired assignment is 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.C74, depends on Storage.C72]  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.C76]  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 unauthorized encryption in transit settings, it should be detected. | Low | Storage.FC1  Storage.FC3 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C56]  Define a diagnostic settings design for Storage Accounts, including destination (tenant/subscription), categories (ideally all), and rotation. 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 their review records. | Low | Storage.FC1  Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | 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)  Storage.T37 (Very Low)  Storage.T41 (Very Low)  Storage.T42 (Very Low)  Storage.T43 (Very Low)  Storage.T51 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C128]  Azure classic Storage Accounts (Azure ASM resources) should not be in use. Azure Cloud Services (classic) will be retired on 31 August 2024. Classic Storage Accounts depend on Azure Cloud Services (classic). They will be retired on the same date. Before that date, you'll need to migrate them to Azure Resource Manager, which has new security features. | Request 1) the mechanism ensuring only authorized Storage Accounts have been deployed using ASM model, 2) its records of execution for all new Storage Accounts, and 3) the plan to move any older Storage Accounts | Very Low | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T5 (Medium)  Storage.T20 (Very Low)  Storage.T21 (Very Low)  Storage.T22 (Very Low)  Storage.T35 (Very Low)  Storage.T36 (Very Low)  Storage.T40 (Very Low)  Storage.T46 (Very High) | Very High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C86, assured by Storage.C87]  Block the usage of the 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.FC1  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)  Storage.T47 (Very High)  Storage.T55 (Very High) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C30, depends on Storage.C29]  Ensure only authorized Groups are used in ACLs for Data Lake Storage Gen2. | Review ACLs against usage of individual users' service principal. | Low | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T34 (Very Low)  Storage.T47 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C36, depends on Storage.C35]  Integrate the access to directories and objects using Azure attribute-based access control [(Azure ABAC)](https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview) in the IAM Operating Model. | 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.T33 (Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C33, depends on Storage.C32]  Use immutable blobs with proper policy. | Ask for immutable policies. Check the usage of immutable blobs. | Medium | Storage.FC2 | Storage.T8 (Very High)  Storage.T9 (Very High)  Storage.T12 (Medium) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C145]  *Preview control* . Prevent the creation of Storage Accounts with allowedCopyScope not set to either AAD or PrivateLink (e.g. by using an Azure Policy in deny/append mode) | Create a storage account with allowedCopyScope not specified (defaults to null), it should be denied | Low | Storage.FC1 | Storage.T57 (Very High) | 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 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)  Storage.T33 (Very Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C98, depends on Storage.C96]  Prevent unauthorized Storage Accounts from having 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.C61]  Maintain a list of authorized blobs and containers with public access level set to anonymous; ideally, none | Request the list of authorized blobs and containers with public access level set to anonymous, its review process, and its review records. | Low | Storage.FC1  Storage.FC2 | Storage.T5 (Very Low)  Storage.T37 (Very Low)  Storage.T50 (Very Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C63, depends on Storage.C61]  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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C43]  Maintain a list of authorized VNETs for the blob, file shares, queues, tables, DFS, NFS, and SFTP access via a 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.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T12 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low)  Storage.T37 (Very Low)  Storage.T43 (Very Low)  Storage.T47 (Very Low)  Storage.T50 (Very Low)  Storage.T55 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C44, depends on Storage.C43, assured by Storage.C46]  Ensure only authorized VNETs are configured for the blob, file shares, queues, tables, DFS, NFS, and SFTP. | Request 1) the mechanism ensuring PE is in place 2) its records of execution for all new DFS. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Low)  Storage.T29 (Low)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T37 (Low)  Storage.T43 (Very Low)  Storage.T47 (Very High)  Storage.T50 (Very Low)  Storage.T55 (Very High) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C45, depends on Storage.C43]  Prevent the use of unauthorized VNETs by the storage account (e.g., by using Azure Policy). | Configure an unauthorized VNET on a storage account, it should be denied. | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very High)  Storage.T3 (Very High)  Storage.T5 (Low)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T37 (Low)  Storage.T43 (Very Low)  Storage.T47 (Very High)  Storage.T50 (Low)  Storage.T55 (Very High) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C46]  Verify the unauthorized VNETs cannot access the storage account. | Configure an unauthorized VNET 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.C48]  Maintain a list of authorized IPs and/or  [resource instance rules](https://azure.microsoft.com/en-gb/updates/storage-resource-instance-rules-ga/) authorized to access each storage account | Request the list of authorized IP or resource instance rules, its review process, and its review records. | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very Low)  Storage.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T9 (Very Low)  Storage.T11 (Very Low)  Storage.T12 (Very Low)  Storage.T15 (Very Low)  Storage.T29 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low)  Storage.T37 (Very Low)  Storage.T43 (Very Low)  Storage.T47 (Very Low)  Storage.T50 (Very Low)  Storage.T55 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C49, depends on Storage.C48, assured by Storage.C51]  Block requests from unauthorized IPs, including trusted services, logging, and metrics read access ([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.T1 (High)  Storage.T3 (High)  Storage.T5 (High)  Storage.T9 (Very Low)  Storage.T11 (Medium)  Storage.T12 (Medium)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T37 (High)  Storage.T43 (Very Low)  Storage.T47 (High)  Storage.T50 (Low)  Storage.T55 (High) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C51]  Verify access is possible only from the 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.C96]  Maintain a list of authorized Storage Accounts that have the static website hosting option enabled; ideally, none | Request the list of authorized Storage Accounts with the 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.C32]  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.C58, depends on Storage.C56]  Ensure Storage Accounts have diagnostic settings configured according to the design. | Create a storage account with unauhorized diagnostic settings options, it should be denied. | Very Low | Storage.FC1  Storage.FC2  Storage.FC7  Storage.FC8  Storage.FC9 | 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)  Storage.T37 (Very Low)  Storage.T41 (Very Low)  Storage.T42 (Very Low)  Storage.T43 (Very Low)  Storage.T51 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C135]  Rewrite every blob created before October 20, 2017. You can force encryption to occur immediately by downloading and re-uploading the blob | Check the creation date. | High | Storage.FC1  Storage.FC2 | Storage.T46 (Medium)  Storage.T49 (Very High) | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C81]  Maintain a list of authorized Azure Storage regions. | Request the list of authorized Azure Storage regions, its review process, and its review records. | Low | Storage.FC1  Storage.FC2  Storage.FC9 | Storage.T13 (Very Low)  Storage.T14 (Very Low)  Storage.T49 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C141, assured by Storage.C143]  Ensure Storage Accounts are created as StorageV2 | 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.FC1 | Storage.T46 (Very Low) | High |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C142, depends on Storage.C141]  Prevent the creation of Storage Accounts that are not StorageV2 (e.g.,by using an Azure Policy in deny mode). | Create a storage account type of BlobStorage or Storagev1, it should be denied. | High | Storage.FC1 | Storage.T46 (Very High) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C143]  Verify all Storage Accounts are of account kind StorageV2 | Create a storage account type of BlobStorage or Storagev1, it should be detected. | Low | Storage.FC1 | - | High |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C26]  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.FC1  Storage.FC2  Storage.FC4  Storage.FC7 | Storage.T3 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T31 (Very Low)  Storage.T32 (Very Low)  Storage.T47 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C31, depends on Storage.C29]  Use name convention for Groups adding Suffix R/RW and Entity to be used. | Review Group-Name convention. | Medium | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T7 (High)  Storage.T9 (Very Low)  Storage.T15 (Low)  Storage.T34 (Very Low)  Storage.T47 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C47]  Use Managed Identity as the method for accessing Azure Storage services. | Check if underlying services are not using SAS or other password methods to authenticate. | Medium | Storage.FC1  Storage.FC2  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T12 (High)  Storage.T47 (Medium)  Storage.T55 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C2]  Define an ACL or IAM authentication for every storage account. Ideally, use Azure AD only and multiple Storage Accounts if fine-grained access is required. | Request the list of all Storage Accounts you control, define their authorized data classification, and 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.T33 (Very Low)  Storage.T34 (Very Low)  Storage.T37 (Very Low)  Storage.T54 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C3, depends on Storage.C2]  Use a data discovery tool (e.g., Microsoft Purview) to control that no sensitive data is stored in an 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.C146]  *Preview control* . Monitor that Storage Accounts with allowedCopyScope set to null / not specified are not created (e.g. using activity logs on "Create/Update Storage Account" operation in ."properties"."requestbody") | Create a storage account with allowedCopyScope set to null, it should be detected | Low | Storage.FC1 | Storage.T57 (Medium) | 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.FC1  Storage.FC2 | Storage.T5 (Very Low)  Storage.T37 (Very Low)  Storage.T50 (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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (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 - "Storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be denied. | High | Storage.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (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 - "Storage account public access should be disallowed"). | Create a storage account with allowblobPublicAccess, it should be detected. | High | Storage.FC1  Storage.FC2 | - | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C55]  Verify Storage Accounts with cross-tenant replication enabled/any Storage Accounts (e.g., using Azure Policy "Storage Accounts should prevent cross tenant object replication" / "allowedCopyScope" parameter in audit mode.). | Create a storage account with cross-tenant/any storage account option enabled, it should be detected. | Low | Storage.FC2  Storage.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C97, depends on Storage.C96, assured by Storage.C99]  Ensure only authorized Storage Accounts has the static website hosting option enabled. | Request 1) the mechanism ensuring only authorized Storage Accounts have the 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.C99]  Verify only authorized Storage Accounts have 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.C14]  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.C52]  Ensure corporate backup policies are implemented for the blob, file shares, queues, tables, and 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)  Storage.T43 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C53]  Maintain a list of objects with cross-tenant or Storage Accounts without private endpoint replication (any storage account) enabled. | Request the list of authorized objects used to allow cross-tenant replication/any Storage Accounts, its review process, and its review records. | Low | Storage.FC2  Storage.FC9 | Storage.T5 (Very Low)  Storage.T13 (Very Low)  Storage.T42 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C54, depends on Storage.C53, assured by Storage.C55]  Ensure cross-tenant replication/any Storage Accounts are allowed only for specific Storage Accounts. | Request 1) the mechanism ensuring any replication allows only authorized Storage Accounts, 2) its records of execution for all new blobs. | High | Storage.FC2  Storage.FC9 | Storage.T5 (High)  Storage.T13 (High)  Storage.T42 (High) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C138, depends on Storage.C139]  Monitor for unauthorized storage account deletions (e.g., using activity log Microsoft.Storage/storageAccounts/delete operation in operationName.value). | Delete a storage account, it should be detected | Medium | Storage.FC1 | Storage.T4 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C139]  Maintain a list of authorized storage account deletions. The process for creating this list should ensure the storage account is not in use. | Request the list of authorized storage account deletions, its review process, and its review records. | Low | Storage.FC1 | Storage.T4 (Very Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C15]  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)  Storage.T39 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C17, depends on Storage.C15]  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.C20, depends on Storage.C15]  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)  Storage.T39 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C37, assured by Storage.C39]  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.T7 (Very Low)  Storage.T9 (Very Low)  Storage.T12 (Very Low)  Storage.T25 (Low)  Storage.T39 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C38]  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)  Storage.T39 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C39]  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.C41, depends on Storage.C37]  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)  Storage.T39 (Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C62, depends on Storage.C61, assured by Storage.C65]  Ensure the 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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C64]  Monitor the creation/update of blobs 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.FC1  Storage.FC2 | Storage.T5 (Medium)  Storage.T37 (Medium)  Storage.T50 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C65]  Verify only authorized blobs 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.FC1  Storage.FC2 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C89]  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.C90, depends on Storage.C89, assured by Storage.C92]  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) its 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.C92]  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 |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C75]  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 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.C131]  Ensure only authorized Azure Files options with security protocol settings are set for authorized Storage Accounts (e.g., using Azure Policy in deny mode utilizing "protocolSettings"/"smb"{"versions","authenticationMethods","kerberosTicketEncryption","channelEncryption":} fields). | Create a file with unauthorized Azure Files security protocol settings for Azure Storage, it should be denied. | Very Low | Storage.FC3 | Storage.T21 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C50, depends on Storage.C48]  Prevent access from unauthorized IPs by allowing only authorized IPs using Azure Storage firewall. | Access from unauthorized IPs, it should be denied. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC7 | Storage.T1 (Very Low)  Storage.T15 (Medium)  Storage.T29 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T47 (Very Low)  Storage.T50 (Low)  Storage.T55 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C57, depends on Storage.C56, assured by Storage.C60]  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.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)  Storage.T37 (Very Low)  Storage.T41 (Very Low)  Storage.T42 (Very Low)  Storage.T43 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C59]  Monitor the creation/update of Storage Accounts with diagnostic settings enabled according to the design (e.g., using activity logs on operation name - create or update resource diagnostic setting) | Configure a storage account with unauthorized diagnostic settings options, it should be detected. | Low | Storage.FC2  Storage.FC8 | Storage.T10 (Medium)  Storage.T41 (Very Low)  Storage.T53 (Very Low)  Storage.T55 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C60]  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.C66]  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.C69, depends on Storage.C66]  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.C70]  Monitor the creation/update and usage of keys for Azure Storage encryption with desired assignment and rotation policy assignment (e.g., using [monitoring](about:blank)) logs on authentication type in AccountKey). | Configure a storage account with an unauthorized encryption setting, it should be detected. | Low | Storage.FC1 | Storage.T14 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C83, depends on Storage.C81]  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.FC2  Storage.FC9 | Storage.T13 (Medium)  Storage.T14 (Very Low)  Storage.T49 (Very Low) | Medium |
| Preventative (COSO)  Detect (NIST CSF) | [Storage.C119]  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)  Protect (NIST CSF) | [Storage.C112]  Periodically scan files with third-party virus scanners that don't only rely on hashes | Request 1) the mechanism ensuring Storage Accounts have been scanned by a third-party tool and 2) its records of execution for all Storage Accounts. | Medium | Storage.FC1  Storage.FC2  Storage.FC3 | Storage.T20 (Medium)  Storage.T35 (Medium)  Storage.T36 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C113, assured by Storage.C115]  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.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium)  Storage.T37 (Low)  Storage.T55 (Very Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C115]  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 |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C140]  Monitor for creation of classic Azure Storage accounts (e.g., using activity log Microsoft.Storage/storageAccounts/writeoperation in operationName.value where properties.requestbody contains either *\"kind\":\"Storage\"* or *"kind\":\"BlobStorage\"*). | Create a BlobStorage and Storagev1 account type, it should be detected. | Medium | Storage.FC1 | Storage.T46 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C136, depends on Storage.C137]  Monitor for unauthorized storage account access key rotations (e.g., using activity log Microsoft.Storage/storageAccounts/regenerateKey/action operation in operationName.value). | Rotate a storage account access key, it should be detected | Medium | Storage.FC7 | Storage.T2 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C137]  Maintain a list of authorized storage account access key rotations. | Request the list of authorized storage account access key rotations, its review process, and its review records. | Low | Storage.FC7 | Storage.T2 (Very Low) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C120]  Maintain a list of authorized Azure Storage SFTP options with authentication methods and permission models. | Request the list of authorized Azure Storage SFTP options with encryption settings, authentication methods, and permission model, its review process, and its review records. | Low | Storage.FC11 | Storage.T44 (Very Low) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C124, depends on Storage.C120]  Ensure only authorized Azure Storage SFTP options with authentication methods and permission models are set for authorized Storage Accounts (e.g., using Azure Policy in deny mode). | Create a blob with unauthorized Azure Storage SFTP options, encryption settings, authentication methods, and permission model for Azure Storage, it should be denied. | Very Low | Storage.FC11 | Storage.T44 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C126]  Do not mix the different services like Azure Files, SFTP, and NFS inside the same Azure Storage account. | Check the configuration of Storage Accounts. | Medium | Storage.FC3 | Storage.T15 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C27, depends on Storage.C26, assured by Storage.C28]  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.FC1  Storage.FC2  Storage.FC4  Storage.FC7 | Storage.T3 (Low)  Storage.T9 (Very Low)  Storage.T12 (Medium)  Storage.T31 (Low)  Storage.T32 (Low)  Storage.T47 (Low) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C28]  Verify SAS tokens only allow authorized IPs. | Deploy a SAS token with an unauthorized IP, it should be detected | Medium | Storage.FC1  Storage.FC2  Storage.FC4  Storage.FC7 | - | Medium |
| Corrective (COSO)  Protect (NIST CSF) | [Storage.C85]  Integrate the access to blob, file shares, queues, tables, and DFS via SAS token (generated from account key and/or user delegation key) in the IAM Operating Model, ideally prioritizing AD as the preferred method. | Check if (Azure) Active Directory is used for assigning permissions. | Medium | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC4  Storage.FC5  Storage.FC7 | Storage.T1 (Low)  Storage.T2 (Low)  Storage.T3 (Low)  Storage.T16 (Very Low)  Storage.T17 (Low)  Storage.T18 (Low)  Storage.T19 (Low)  Storage.T27 (Low)  Storage.T28 (Low)  Storage.T47 (Low)  Storage.T55 (Low) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Storage.C4]  Use a data discovery tool (e.g., Microsoft Purview) 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.C144, assured by Storage.C147]  *Preview control* . Ensure Storage Accounts have allowedCopyScope set to either AAD or PrivateLink | Request 1) the mechanism ensuring only authorized Storage Accounts are configured, 2) its records of execution for all new Storage Accounts, and 3) the plan to update unauthorized Storage Accounts | High | Storage.FC1 | Storage.T57 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C147]  *Preview control* . Verify Storage Accounts with allowedCopyScope set to null, are not configured (e.g. by using an Azure Policy in audit mode) | Create a storage account with allowedCopyScope set to null, it should be detected | Medium | Storage.FC1 | - | 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)  Storage.T40 (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)  Protect (NIST CSF) | [Storage.C12, assured by Storage.C13]  Enable snapshots to Azure Files holding primary data | Request the mechanism used to ensure snapshots to Azure Files on blobs holding primary data and its records | Medium | Storage.FC2 | Storage.T7 (Low)  Storage.T40 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C13]  Verify Azure Files have snapshots configured as an alternative to the versioning. | Remove snapshots from an Azure Files account holding primary data, it should be detected | High | Storage.FC2 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C77]  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.C79, depends on Storage.C77]  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.C40, assured by Storage.C42]  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)  Storage.T39 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C42]  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.C91, depends on Storage.C89]  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)  Identify (NIST CSF) | [Storage.C22]  Maintain a list of authorized Storage Accounts with the 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.T40 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C23, depends on Storage.C22, assured by Storage.C24]  Ensure only authorized Storage Accounts with the 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 the hierarchical namespace (DFS) option enabled. | Medium | Storage.FC2 | Storage.T6 (Low)  Storage.T7 (Low)  Storage.T40 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C24]  Verify Storage Accounts with the 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 the hierarchical namespace (DFS) option enabled, it should be detected | Medium | Storage.FC2 | - | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C71]  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 setting, it should be detected. | High | Storage.FC1 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C104]  Maintain a list of authorized NFS/SMB 2.1 Azure Files. | Request the list of authorized NFS/SMB 2.1 Azure Files with NFS/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.C105, depends on Storage.C104, assured by Storage.C108]  Ensure only authorized Azure Files NFS/SMB 2.1 have encryption disabled. | Request 1) the mechanism ensuring only authorized NFS/SMB 2.1 Azure Files have encryption disabled, 2) its records of execution for all new NFS/SMB 2.1 Azure Files, and 3) a plan to move any older Storage Accounts | High | Storage.FC3 | Storage.T21 (Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C106, depends on Storage.C104]  Prevent unauthorized Azure Files NFS/SMB 2.1 from having 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.C107]  Monitor the creation/update of Azure Files NFS/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.C108]  Verify only authorized Azure Files NFS/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 |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C129]  Maintain a list of authorized Azure Files security protocol settings (ideally maximum security SMB 3.1.1, Kerberos, AES-256 only). | Request the list of authorized Azure Files security protocol settings, its review process, and its review records. | Low | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C130, depends on Storage.C129, assured by Storage.C132]  Ensure authorized Azure Files options with security protocol settings are set for authorized Storage Accounts. | Request 1) the mechanism ensuring only Azure Files security protocol settings for Storage Accounts are in use, 2) its records of execution for all new Storage Accounts, and 3) the plan to move any older Storage Accounts. | High | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C132]  Verify only authorized Azure Files options with security protocol options are set for authorized Storage Accounts (e.g., using Azure Policy on audit mode utilizing "protocolSettings"/"smb"{"versions","authenticationMethods","kerberosTicketEncryption","channelEncryption":} fields). | Configure a storage account with an unauthorized Azure Files security protocol settings model, it should be detected. | High | Storage.FC3 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C133]  Refrain from mixing or downgrading security options for the Azure Files shared inside the same Azure Storage account. | Check the configuration of Storage Accounts (Azure Files). | Medium | Storage.FC3 | Storage.T21 (Very Low) | Low |
| Detective (COSO)  Protect (NIST CSF) | [Storage.C88]  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 an unauthorized or default quota, it should be detected. | Very Low | Storage.FC3 | Storage.T16 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C67, depends on Storage.C66, assured by Storage.C71]  Ensure authorized keys for Azure Storage encryption with desired assignment and rotation policy are 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) the plan to move any older Storage Accounts | High | Storage.FC1 | Storage.T14 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C68]  Protect Key Vault store custom encryption keys using Key Vault ThreatModel. | Check settings for Key Vault. | High | Storage.FC1 | Storage.T38 (Medium) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C134]  Maintain a list of blobs created before October 20, 2017 (ideally none). | Request 1) the list of blobs created before October 20, 20017, 2) its records of execution for rewriting, and 3) the plan to rewriting. | Low | Storage.FC1  Storage.FC2 | Storage.T46 (Very Low)  Storage.T49 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C82, depends on Storage.C81, assured by Storage.C84]  Ensure the authorized Azure Storage region is set for authorized Storage Accounts. | Request 1) the mechanism ensuring only Azure Storage authorized regions 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.FC2  Storage.FC9 | Storage.T13 (Very Low)  Storage.T14 (Very Low)  Storage.T49 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C84]  Verify only the authorized Azure Storage region is set for authorized Storage Accounts (e.g., using Azure Policy on audit mode). | Create a storage account with an unauthorized Azure Storage region, it should be detected. | High | Storage.FC1  Storage.FC2  Storage.FC9 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C121]  Integrate the access to SSH in the IAM Operating Model, including monitoring of creating local SSH users. | Request the IAM Operating Model for SSH access. | Low | Storage.FC11 | Storage.T44 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C122]  Use SSH private key credentials for authentication as the preferred authentication method. | Check the usage of local passwords in SFTP-enabled accounts. | Medium | Storage.FC11 | Storage.T44 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C109, assured by Storage.C111]  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.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low)  Storage.T37 (Very Low)  Storage.T55 (Very Low) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C110]  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.T3 (Very Low)  Storage.T5 (Low)  Storage.T20 (Medium)  Storage.T37 (Very Low)  Storage.T55 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C111]  Verify all Storage Accounts have Azure Defender for storage account enabled | Create a storage account without Azure Defender for storage, it should be detected. | Low | Storage.FC2  Storage.FC3  Storage.FC7 | - | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Storage.C114, depends on Storage.C109]  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.T3 (Very Low)  Storage.T5 (Very Low)  Storage.T20 (Very Low)  Storage.T37 (Very Low)  Storage.T55 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C127]  The latest (or latest -1 with no security vulnerabilities) non-preview version of storage software libraries must be used for Storage Accounts. Running on older versions could mean you are not using the latest security classes. Usage of such old classes and types can make your application vulnerable. | Check the software libraries that are in use for Storage Accounts. | Very High | Storage.FC1  Storage.FC3 | Storage.T21 (Low)  Storage.T45 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C123, depends on Storage.C120, assured by Storage.C125]  Ensure authorized Azure Storage SFTP options with authentication methods and permission models are set for authorized Storage Accounts. | Request 1) the mechanism ensuring only Azure Storage SFTP options with encryption settings, authentication methods, and permission model for Storage Accounts are in use, 2) its records of execution for all new Storage Accounts, and 3) the plan to move any older Storage Accounts. | High | Storage.FC11 | Storage.T44 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C125]  Verify only authorized Azure Storage SFTP options with authentication methodsand permission models are set for authorized Storage Accounts (e.g., using Azure Policy on audit mode). | Configure a storage account with unauthorized SFTP options, encryption settings, authentication methods, and permission models, it should be detected. | High | Storage.FC11 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Storage.C93]  Maintain a revocation plan for any SAS or storage account access keys issued to clients based on requirements. If a SAS is compromised, you must revoke that SAS as soon as possible. To revoke a user delegation SAS, revoke the user delegation key to 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)). To revoke a storage account access key, regenerate the key. | Request the authorized revocation plan for any SAS or storage account access keys, its review process, and its review records. | Low | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low)  Storage.T47 (Very Low)  Storage.T55 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C94, depends on Storage.C93, assured by Storage.C95]  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.FC1  Storage.FC2  Storage.FC3  Storage.FC7 | Storage.T1 (Very Low)  Storage.T2 (Very Low)  Storage.T3 (Very Low)  Storage.T16 (Very Low)  Storage.T47 (Very Low)  Storage.T55 (Very Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C95]  Verify the revocation plan is in place for any SAS or storage account access key. | Check test executions. For any unsuccessful attempts, it should be detected | High | Storage.FC1  Storage.FC2  Storage.FC3  Storage.FC7 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C78, depends on Storage.C77, assured by Storage.C80]  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.C80]  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 setting, it should be detected. | High | Storage.FC1 | - | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Storage.C16, depends on Storage.C15, assured by Storage.C18]  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.C18]  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.C19, depends on Storage.C15, assured by Storage.C21]  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)  Storage.T39 (Very Low) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Storage.C21]  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)  Identify (NIST CSF) | [Storage.C100]  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.C101, depends on Storage.C100, assured by Storage.C103]  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.C102, depends on Storage.C100]  Prevent unauthorized Storage Accounts from using 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.C103]  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.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/clearLegalHold/action | TODO | ClearblobContainerLegalHold |
| Storage.A26 | Set blob container legal hold | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/setLegalHold/action | TODO | SetblobContainerLegalHold |
| Storage.A27 | Extend blob container immutability policy | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/extend/action | TODO | ExtendblobContainerImmutabilityPolicy |
| Storage.A28 | Delete blob container immutability policy | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/delete | TODO | DeleteblobContainerImmutabilityPolicy |
| Storage.A29 | Put blob container immutability policy | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/write | TODO | PutblobContainerImmutabilityPolicy |
| Storage.A30 | Lock blob container immutability policy | Storage.FC2 | Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/lock/action | TODO | LockblobContainerImmutabilityPolicy |
| Storage.A31 | Get blob container immutability policy | Storage.FC2 | 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.FC6 | 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.FC11 | Microsoft.Storage/storageAccounts/localUsers/delete | TODO | DeleteLocalUser |
| Storage.A125 | List local user keys | Storage.FC11 | Microsoft.Storage/storageAccounts/localusers/listKeys/action | TODO | ListLocalUserKeys |
| Storage.A126 | List local users | Storage.FC11 | Microsoft.Storage/storageAccounts/localusers/read | TODO | ListLocalUsers |
| Storage.A127 | Get local user | Storage.FC11 | Microsoft.Storage/storageAccounts/localusers/read | TODO | GetLocalUser |
| Storage.A128 | Create or update local user | Storage.FC11 | 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 |